Contract NAS5-32605

EOSDIS IV&V

EOSDIS TEST VERSION
COMPONENT ACCEPTANCE TEST PROCEDURES
FOR
ECS IR1

Baseline
(Deliverable 1004 Task 10C)

January 15, 1996

Prepared by:

INTERMETRICS
6301 Ivy Lane, Suite 200
Greenbelt, MD 20770

Prepared for:

NASA Goddard Space Flight Center
Code 505
Greenbelt, MD 20770

This page intentionally left blank

Contract NAS5-32605

EOSDIS IV&V

EOSDIS TEST VERSION
COMPONENT ACCEPTANCE TEST PROCEDURES
FOR
ECS IR1

Baseline
(Deliverable 1004 Task 10C)

January 15, 1996

SUBMITTED BY:

Gordon Henley
Task Lead

APPROVED BY:

Frank Rockwell
EOSDIS IV&V Program Manager

APPROVED BY:

Darryl Lakins
ESDIS Project
IV&V COTR

INTERMETRICS
6301 Ivy Lane, Suite 200
Greenbelt, MD 20770

This page intentionally left blank

Purpose

This document supplies the test procedures to implement the EOSDIS Test Version Component Acceptance Test (AT) program described in the EOSDIS Test Version Component Acceptance Test Plan (IV&V Contractor Deliverable 1003).

The EOSDIS Test Version Component AT Program is organized into four test categories comprised of 32 tests. For each test, the following is provided:

- A brief description of the test and the test objectives
- Test Configuration specifications
- Test Data listings
- Test Procedures, including steps for test set-up, test execution, post-test analysis, test termination and expected results

TABLE OF CONTENTS

Section ***Page***

TABLE OF EXHIBITS

Section ***Page***

1.0 Applicable Documents

1.1 Parent Documents

(1) Component Acceptance Master Test Plan
(Deliverable 1002) INTERMETRICS, 06 October, 1995

(2) EOSDIS Test Version Component Acceptance Test Plan, Baseline
(Deliverable 1003) INTERMETRICS, 03 November, 1995

(3) EOSDIS Test Version Component Acceptance Test Procedures for ECS IR1, Preliminary (Deliverable 1004) INTERMETRICS, 01 December, 1995

(4) EOSDIS Test Version Component Acceptance Test Procedures for ECS IR1, Review (Deliverable 1004) INTERMETRICS, 15 December, 1995

1.2 Operational Documents

(1) Interim Release One (Ir1) Maintenance and Operations Procedures
(609-CD-001-001) HITC, December 1995

(2) Operators Manual for the ECS Project
(611-CD-001-001) HITC, December 1995

(3) Interim Release One (Ir1) Integration and Test Plan and Procedures
(322-CD-001-002, 414-CD-001-002) HITC, December 1995

1.3 Test Thread Revisions

Several test threads delineated in the EOSDIS Test Version Component Acceptance Test Plan for ECS IR1 (November 3, 1995) have been revised. The modifications optimize Component AT test threads and procedures, and yet address all IR1 requirements. Requirement mappings have been updated to reflect the modified procedures. The following table denotes these changes.

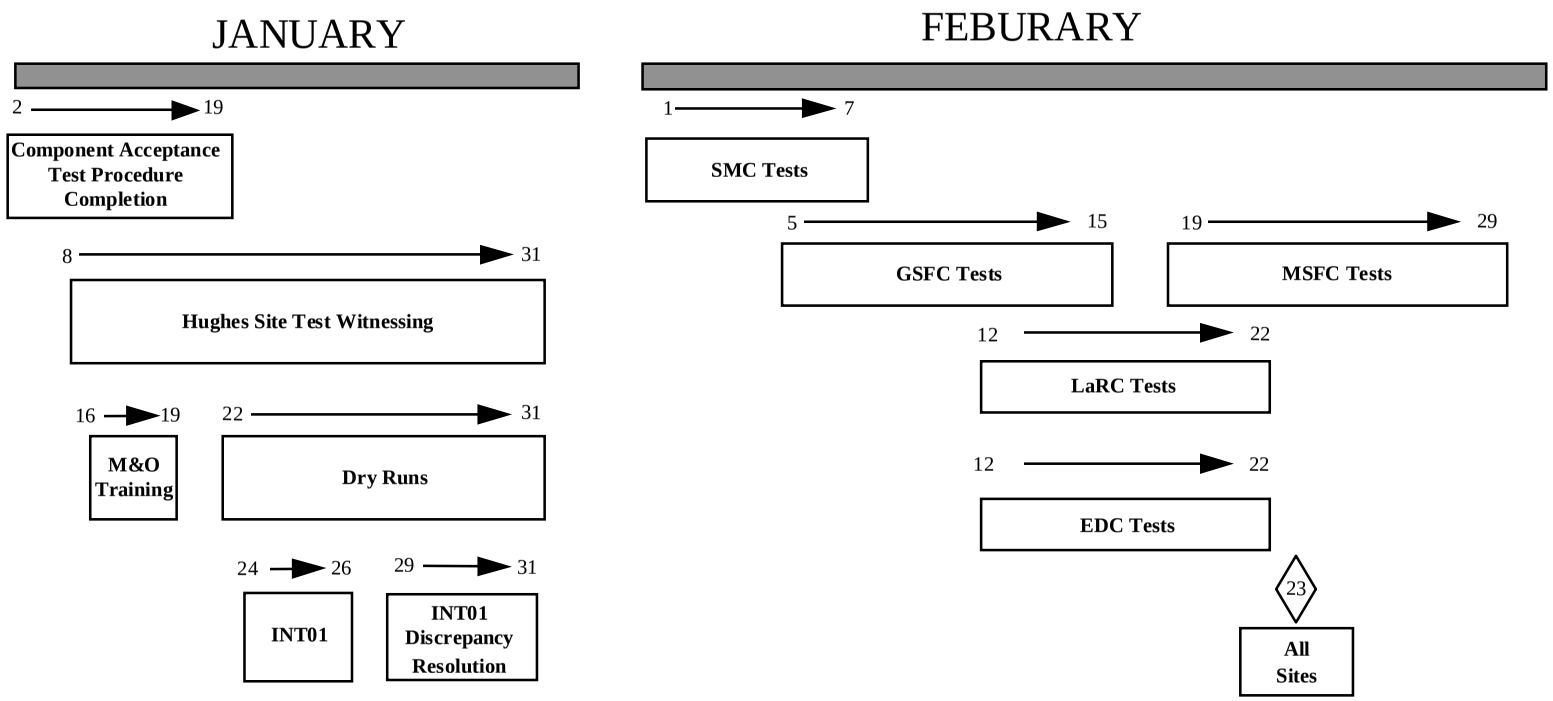
Comp. AT Plan	Comp. AT Procedures	Change
CFT01.3	CFT01.3	The scope of this test was modified to reflect the implementation of the configuration management tool.
CFT02		This test was removed with functionality going to CFT01, INT01 and the new SFT05
EXT01.3 EXT02.4		These tests are accounted for in EXT03.2.
EXT01.2		These tests were removed due to no automatic validation of the

Comp. AT Plan	Comp. AT Procedures	Change
EXT02.3 EXT03.2		ingest function being performed in IR1.
	EXT01.2 EXT02.3	These test cases were added to handle ingest error conditions.
	INT01.3 INT01.4	These tests were added to inspect and analysis protocol and policy and procedures.
INT02		This test was removed with functionality transferred to SFT02.
SFT02.4	INT01.4	This test was moved to INT01.4.
SFT03.3	INT01.3	This test was moved to INT01.3.
SFT05		This test was merged with SFT02.
SFT06	SFT05	Since SFT05 was removed, SFT06 was renamed to SFT05.

EXHIBIT 1-1: UPDATES

2.0 Component AT Schedule

The following exhibit depicts the schedule presented in the Component Acceptance Test Plan for ECS Ir1 in a pictorial format. This information is presented again with the procedures so that each facility may examine the schedule of acceptance testing at their location. Details of this schedule will continue to be coordinated within the ESDIS organization and with the DAACs involved in Ir1 testing.



Dry Runs

During this time interval the testers will have access to the system in order to perform dry runs of tests to finalize procedures.

INT01

During this time interval an analysis/inspection of all software, hardware, and procedures at each site will be conducted. This test will be performed prior to the other component tests beginning. Any errors or discrepancies found during this test will need to be answered/explained prior to the beginning of testing at the SMC.

INT01 Discrepancy Resolution

This time interval is set aside to resolve any discrepancies from the analysis in the INT01 test.

SMC Tests

During this time interval one day will be allotted for each of the following tests *:
SFT03 / SFT04 / SFT01 / SFT02 / SFT05

GSFC Tests

During this time interval one day will be allotted for each of the following tests *:
SFT03 / SFT04 / SFT01 / SFT02 / SFT05/CFT01 / EXT01 / EXT02 / EXT03

LaRC Tests

During this time interval one day will be allotted for each of the following tests *:
SFT03 / SFT04 / SFT01 / SFT02 / SFT05/CFT01 / EXT01 / EXT02 / EXT03

EDC Tests

During this time interval one day will be allotted for each of the following tests *:
SFT03 / SFT04 / SFT01 / SFT02 / SFT05/CFT01 / EXT01 / EXT02 / EXT03

MSFC Tests

During this time interval one day will be allotted for each of the following tests *:
SFT03 / SFT04 / SFT01 / SFT02 / SFT05/CFT01 / EXT01 / EXT02 / EXT03

***All Site Test** - During the interval when there are testers at all sites, a test from SFT02 will be run which verifies the ability of the SMC to detect faults/failures at all sites.

Test Teams:

The test teams will be divided into three groups. Team A, B and C will be involved with INT01, the SMC tests and the beginning of the GSFC tests. Then team B and C will travel to LaRC and EDC. Team A will conduct the MSFC tests at the conclusion of GSFC tests.

EXHIBIT 2-1: Schedule

4.0 TEST PROCEDURES

Each test is organized as follows:

- Test Objectives - Defines the functionality being verified in the test thread. Each test case verifies at least one of the objectives stated in this section.
- Test Configuration - Defines the hardware, software, and test tools necessary to execute the test cases within the thread.
- Test Data Description - Defines the data necessary to run the test. The data will be gathered and marked according to the test cases prior to execution.
- Requirements Verified - Lists all the Level 3 requirements, by criticality rating, being verified in the test thread. Each test case will verify at least one of the listed requirements.
- Procedures - Contains the actual steps for performing the test. The procedures are organized as follows:

    1. Test Set-up - Contains pre-test information necessary to run the test cases within the thread. Pre-test information includes account names, data path names, list of delivered components, expected results, etc. All of the steps in this section must be completed prior to test execution.
    2. Test Execution - Contains the steps necessary to run each test case, along with expected results.
    3. Post Test Analysis - Contains any off-line analysis necessary for requirements verification. Information including report verification, history log analysis, expected results, etc. is listed in this section.
    4. Test Termination - Contains steps to perform upon completion of the test thread and prior to exiting the testing environment.

This document does not address the following areas:

- Test tool definition and operational procedures (especially simulators)
- Sources of test data, including:

    1. Data for ingest into the system
    2. Science software delivery packages to use in the validation of the science software integration process to include algorithms, calibration coefficients, expected results and associated documentation
    3. Data sets for use in file transfers between DAACs
    4. Data to be used for error and exception handling
    5. Data search parameters

- System performance parameters such as:

    1. Time out periods
    2. System threshold values, including:
        - Data search criteria

- Information regarding the simulation of system faults

This information is being obtained during HITC test witnessing, training, and Component Acceptance Test dry runs.

4.1 CFT01 - Science Software Integration and Operations

Test Objectives:

This test verifies the capability of ECS at the DAACs to receive, integrate, and execute science software. It also verifies monitoring and configuration management of the science software. Specific objectives to be tested are:

- Receipt of algorithm and calibration coefficients from SCF.
- Algorithm validation.
- Algorithm execution, monitoring, and result reporting.
- Algorithm configuration management.
- Algorithm update.

Test Configuration:

- Hardware: AI&T Server and Workstation.
- Software: AITTL.
- Test Tools: None.

Test Data:

Test Data	File Name / Location
Science S/W Delivery Package (FORTRAN 77, without errors)	
Science S/W Delivery Package ("C", without errors)	
Science S/W Delivery Package (Ada, without errors)	
Science S/W Delivery Package (FORTRAN 77, with errors)	
Calibration Coefficient file (without errors)	
Calibration Coefficient file (with compile errors)	

Requirements Verified:

Mission Essential:

DADS0190	DADS2450	EOSD0500	EOSD0730	EOSD1703	EOSD1750
ESN-0006	PGS-0270	PGS-0360	PGS-0370	PGS-0400	PGS-0602
PGS-0610	PGS-0620	PGS-0640	PGS-0650	PGS-0860	PGS-0900
PGS-0910	PGS-0920	PGS-0925	PGS-0940	PGS-0950	PGS-0970
PGS-0980	PGS-0990	PGS-1000	PGS-1010	PGS-1220	PGS-1315
SDPS0010	SDPS0090				

Mission Fulfillment:
EOSD1760 EOSD5020

Procedures:

Test Set-up:

Step	Action	Expected Results	Comments
1.	Acquire two valid account names and passwords for the ECS.	Account / Password combinations received.	
2.	Verify that a VOB and a view have been created for use by ClearCase.	View name: _____ VOB path: _____	
3.	Logon to the ECS at the DAAC using a valid account and password.	System allows access.	
4.	At the DAAC Enter: <**script CFT01_DAAC.log**>. Initiates UNIX script file to record test history.		
5.	Log onto the ECS at the SCF using a valid account and password.	System allows access.	
6.	At the SCF Enter: <**script CFT01_SCF.log**>. Initiates UNIX script file to record test history.		

Test Execution:

CFT01.1 Receipt of Science Software Delivery Package and/or Calibration Coefficients

This test case verifies receipt of science software delivery package and calibration coefficients.

Step	Action	Expected Results	Comments
1.	SCF coordinates with the DAAC. The SCF shall send the Science Software delivery package to the DAAC at the agreed upon anonymous drop off point.		The SCF is pushing the file.
2.	SCF transfer the Science Software delivery package to DAAC through manual file transfer (ftp). Perform a file compare of the Science Software delivery package in the DAAC directory with the original file selected for transfer at the SCF. The files should be identical. Verify that the DAAC's Science Software delivery package contains the following: a._Algorithm identification b._Algorithm source code c._List of required inputs d._Processing dependencies e._Test data and procedures f._Algorithm documentation	File transferred successfully. Both files are identical. All required information incorporated.	
3.	Delete the Science software delivery package at the DAAC.	File deleted.	

Step	Action	Expected Results	Comments
4.	Coordinate with the SCF via phone. The DAAC shall retrieve the Science Software delivery package from the SCF at the agreed upon anonymous drop off point.		
5.	DAAC retrieve Science Software delivery package from SCF through manual file transfer (ftp). Verify that the DAAC's Science Software delivery package file date, time, and size are the same as the original SCF file.	Files transferred successfully. Both files are identical.	
6.	Extract Science Software delivery package tarfile using the following command Enter: "**uncompress -c <tarfile>**".	Files extracted.	
7.	Coordinate with the SCF via phone. The SCF shall send the calibration coefficient update package to the DAAC.		

Step	Action	Expected Results	Comments
8.	SCF transfer calibration coefficient update package to DAAC through manual file transfer (ftp). Verify that the DAAC's calibration coefficient file date, time, and size are the same as the original SCF file Verify that the DAAC's calibration coefficient file contains the following information: a._Identification of coefficient data set b._Calibration coefficients values c._Author and version number d._Identification of related processing algorithm e._Start and stop date/time of applicability f._Date and time g._SCF identification h._Reasons for update	Files transferred successfully. Both files are identical. All required information incorporated.	

Post Test Analysis:

No post test analysis is necessary for this test.

CFT01.2 SCF Algorithm and Calibration Coefficient Validation

This test case verifies algorithm and calibration coefficient validation . This test case is run at each DAAC on each platform (HP, SUN, SGI), utilizing the appropriate Science Software Delivery Package.

Step	Action	Expected Results	Comments
1.	Compile a valid FORTRAN 77 algorithm from a valid Science Software Delivery Package	Successful compile.	
2.	Verify date & time of compiled file.	Current date & time.	
3.	Attempt to compile a FORTRAN 77 algorithm with the calibration coefficient file containing compile errors.	Error detected and displayed; events logged.	
4.	At the SCF, receive notification of problems with Calibration Coefficient Package.	Notification received.	
5.	Compile a valid “C” algorithm from a valid Science Software Delivery Package	Successful compile.	
6.	Verify date & time of compiled file.	Current date & time.	
7.	Compile a valid Ada algorithm from a valid Science Software Delivery Package (LaRC only)	Successful compile.	
8.	Verify date & time of compiled file.	Current date & time.	

Post Test Analysis:

No post test analysis is necessary for this test.

CFT01.3 Algorithm and Calibration Coefficient Configuration Management

This test case verifies Algorithm and Calibration Coefficient Configuration Management.

Step	Action	Expected Results	Comments
1.	At the AIT workstation at the DAAC, open the ClearCase working view.	The working view is started.	
2.	Change the current directory to the VOB where the algorithm and calibration coefficient files are to be placed.	Directory changed.	
3.	Check in a copy of a valid algorithm, and valid calibration coefficient file. Verify that the following information is available for the algorithm under CM control: 1) Source code including version number and author 2) Benchmark test procedures 3) Date and time of operational installation 4) Compiler identification and version 5) Final algorithm documentation	Files checked in. Information available for the algorithm is under CM control.	
4.	Check out the algorithm under configuration control.	Files checked out.	
5.	Edit the algorithm. (Make any type of change.)	File changed.	
6.	Save the changes.	File saved.	
7.	Check in the edited algorithm.	File checked in.	

Step	Action	Expected Results	Comments
8.	Verify that the date and time of the newly checked in algorithm reflects the time of the editing. Verify that the following information, available for the calibration coefficient file under CM control, has been updated as appropriate: 1) Source code including version number and author 2) Benchmark test procedures 3) Date and time of operational installation 4) Compiler identification and version 5) Final algorithm documentation	Date and time are recent. Information available for the calibration coefficient file is under CM control.	
9.	Attempt to edit and save the calibration coefficient file without "checking it out".	Will not allow access to file or will not overwrite original file.	
10.	Exit ClearCase view.		

Post Test Analysis:

No post test analysis is necessary for this test.

CFT01.4: Algorithm Execution and Monitoring

This test case verifies Algorithm Execution and Monitoring.

Step	Action	Expected Results	Comments
1.	Start Autosys Enter:"**autosys &**".	Autosys GUI control panel displayed.	
2.	Activate the Autosys Job Activity Console Enter:"**autocons &**".	Job Activity Panel displayed.	
3.	Enter the Job Definition menu.	Job Definition dialog appears.	

Step	Action	Expected Results	Comments
4.	Note: Steps 4 - 12 describe the process of submitting an algorithm for processing. Subsequent algorithm execution steps will refer to the process as simply "**Submit <algorithm> for execution via Autosys, under job name <job name**>."		
5.	Enter:"**CFT014a**" in the Job Name field.	Information entered.	
6.	Enable the "**Command**" button in the Job Type field.	Button highlighted.	
7.	In the "**Execute on Machine**" field, enter the name of the machine on which the command will be executed.	Information entered.	
8.	In the UNIX command field, enter the name of the algorithm to be executed.	Information entered.	
9.	Click on the "**save**" button in the Job Definition dialog box.	Button highlighted.	
10.	Click on the "**Send Event**" button on the Autosys control panel.	Button highlighted	
11.	Enter "**startjob**" in the Type of Event name field.	Information entered.	
12.	In the Job Name field, enter "**CFT014a**" as the job's name.	Information entered.	
13.	Click on the "**Execute**" button.	Observe job execution status on the Job Activity Panel.	
14.	Submit algorithm #2 (with errors) for execution via Autosys, under job name CFT014b.	Observe job execution status on the Job Activity Panel. Errors detected and displayed.	
15.	Prepare a software problem report using MS WORD, regarding the errors found. Send to appropriate SCF.	Report sent.	

Step	Action	Expected Results	Comments
16.	At the SCF, receive software problem report notification of invalid algorithm.	Notification received and is readable.	
17.	Submit algorithm #3 (with calibration coefficient errors) for execution via Autosys, under job name CFT014c.	Observe job execution status on the Job Activity Panel.	
18.	Compare algorithm test results at the DAAC with the delivery package sample results. Verify out of threshold differences identified.	Out of threshold differences identified. Proper out of threshold differences listed.	
19.	Send test products to SCF for analysis. Verify test products sent to SCF contain: 1) Algorithm identification 2) Test time(s) 3) Processor identification 4) Test results.	Files successfully transferred. All components included.	
20.	Submit algorithm #1 and algorithm #3 for execution via Autosys, under job names CFT014d and CFT014e respectively.	Observe job execution status on the Job Activity Panel.	
21.	Highlight job CFT014e and place it "**On Hold**".	"On Hold" appears in the status field.	
22.	After job CFT014d completes successfully, verify that CFT014e does not execute.	CFT014e status remains on hold.	
23.	Highlight job CFT014e and place it "**Off Hold**".	CFT014e status changes to starting and eventually successful.	
24.	Submit algorithm #1 for execution via Autosys, under job name CFT014f.	Observe job execution status on the Job Activity Panel.	

Step	Action	Expected Results	Comments
25.	After CFT014f has started, highlight the job and "**Kill Job**".	Status changes to Kill job and alarm button turns red.	
26.	Reset, then cancel the alarm.	Alarm manager window is displayed.	
27.	Close Autosys windows.		

Post Test Analysis:

No post test analysis is necessary for this test.

Test Termination:

Step	Action	Expected Results	Comments
1.	Print both local and remote history logs (UNIX script files).		
2.	Log off both local and remote sessions.		

4.2 EXT01 - TRMM Level 0 Data Ingest from SDPF

Test Objectives:

This test verifies the capability of ECS at the DAACs to receive and ingest TRMM (CERES and LIS) Level 0 data from the SDPF. Nominal ingest and error and exception handling are verified.

This test is executed twice:

Run 1: SDPF simulator at EDF transmitting to MSFC DAAC
Run 2: SDPF simulator at EDF transmitting to LaRC DAAC

Test Configuration:

- Hardware: Ingest Server.
- Software: INGST, DCCI, INCI CSCIs.
- Test Tools: SDPF Simulation.

Test Data:

Test Data	File Name / Location
Level 0 Data (simulated file)	ext01_level_0.dat
Level 0 data (simulated files) to exercise multiple products in the queue.	ext01_level_0_1.dat ext01_level_0_2.dat ext01_level_0_3.dat

Requirements Verified:

Mission Essential:
DADS0130 DADS0145 DADS0250 DADS1070 DADS1380 DADS1400
EOSD0500 EOSD0730 EOSD1607 EOSD1608 ESN-0070 SDPS0020
SDPS0080 SDPS0110

Mission Fulfillment:
EOSD5020

Procedures:

Test Set-up:

Step	**Action**	**Expected Results**	**Comments**
1.	Log in as DAAC operator		
2.	Open a UNIX script file to maintain test history. Enter: **script**<**filename**>	Record filename below: _____	
3.	Check in with SDPF simulator at EDF, verify ready to support test.		

Test Execution:

EXT01.1 Transfer of TRMM L0 Data from GSFC SDPF

Step	Action	Expected Results	Comments
1.	Logon to the DAAC Ingest Server and Gateway Server workstations. Enter:<**login id**> Enter:<**password**>		For in house testing the EDF DAAC Ingest and Gateway Servers and will act as the Ingest and Gateway Servers for all DAACs.
2.	Start the Gateway and Ingest Server processes if they are not currently running. You must **dce_login** prior to starting the Ingest Server process.		
3.	On the DAAC Ingest workstation set the "**DAA message option**" to "**Accepted**" and the "**DDN message option**" to "**Successful**".		
4.	Remote logon to the simulated Data Provider (SDPF) workstation three times using three xterm's.		
5.	On the second xterm change directory to the SDPF simulator executable directory and then start up the simulator user interface.		
6.	On the first xterm change directory to the SDPF simulator executable directory and then start up the simulator.		
7.	On the third xterm window configure the correct authentication request file (valid) for the LaRC DAAC.		
8.	On the first xterm send a	Successful transmission of	

Step	Action	Expected Results	Comments
	valid Authentication Request to the LaRC DAAC.	Authentication Request.	
9.	On the second xterm, after receiving the Authentication Response send valid LDAN-2 to the LaRC DAAC.	Successful transmission of LDAN-2.	LDAN-2 contains CERES L0 (data & SFDU) and TRMM Predictive & Definitive 0rbit data.
10.	After the DAAC Ingest Server receives the DDA get a printout of the DDN, the DAA, and the Authentication Response using the third xterm and then delete all messages.	The Authentication Response should indicate that your Authentication Request was accepted. The DAA should indicate that LDAN-2 was accepted. The DDN should indicate that the data was transferred successfully.	Use the parser tool 'prtm' to get the Authentication Response, DAA and DDN in ASCII form.
11.	On the DAAC Ingest Server workstation, printout the Event Log.	The Event Log should contain entries for all of the ingest messages.	
12.	On the DAAC Ingest Server workstation, printout a listing of the temporary storage directory.	The listing of the temporary storage directory should contain all files identified in LDAN-2.	
13.	On the second xterm shutdown the simulator.		
14.	On the second xterm start up the simulator user interface.		
15.	On the first xterm start up the simulator.		
16.	On the third xterm window configure the correct authentication request file (valid) for the MSFC DAAC.		
17.	On the first xterm send a valid Authentication Request to the MSFC DAAC.	Successful transmission of Authentication Request.	
18.	On the second xterm, after receiving the	Successful transmission of MDAN-2.	MDAN-2 contains LIS L0 (data SFDU) and

Step	Action	Expected Results	Comments
	Authentication Response send valid MDAN-2 to the MSFC DAAC.		TRMM Predictive & Definitive 0rbit data.
19.	After the DAAC Ingest Server receives the DDA get a printout of the DDN, the DAA, and the Authentication Response using the third xterm and then delete all messages.	The Authentication Response should indicate that your Authentication Request was accepted. The DAA should indicate that MDAN-2 was accepted. The DDN should indicate that the data was transferred successfully.	Use the parser tool 'prtm' to get the Authentication Response, DAA and DDN in ASCII form.
20.	On the DAAC Ingest Server workstation, printout the Event Log.	The Event Log should contain entries for all of the ingest messages.	
21.	On the DAAC Ingest Server workstation, printout a listing of the temporary storage directory.	The listing of the temporary storage directory should contain all files identified in MDAN-2.	
22.	On the DAAC Ingest Server workstation, printout a listing of the temporary storage directory.	The listing of the temporary storage directory should contain all files identified in MDAN-2.	
23.	On the DAAC Ingest workstation delete all files that may reside in the temporary storage directory. Enter: **rm -f /Ir1_IT/INGEST/temp_store/***		
24.	Logoff all xterm's and then logoff the DAAC Ingest and Gateway Server workstations. End test.		

Post Test Analysis:

No post test analysis is necessary for this test.

EXT01.2 Error and Exception Handling

Step	Action	Expected Results	Comments
1.	ECS transmits the following authentication requests to the SDPF, in sequence, waiting for the response from the SDPF before transmitting the next request. Verify that an error message is displayed to the operator and/or event log as indicated. 1) (request filename - TBD)	"Invalid message type" type = 50d	Note: This also verifies that the router rejects DANs with invalid message types.
2.	ECS transmits a valid authentication message to the SDPF.	Socket connection to ECS established.	
3.	SDPF transmits the following invalid DANs to the GSFC DAAC. (1) (filename - TBD)	A short DAA is received from ECS with the following errors: Invalid DAN sequence number (SEQ_NO = -3)	

Post Test Analysis:

No post test analysis is necessary for this test.

Test Termination:

Step	Action	Expected Results	Comments
1.	Print the test history file (UNIX script file)		
2.	Print the MSS Event Log.		
3.	Take down the SDPF simulator at the EDF.		

4.3 EXT02 - ECS - TSDIS Interface Test

Test Objectives:

This test verifies the capability to

- Transfer data from TSDIS to ECS at the GSFC DACC via the DAN/DAA protocol.
- Transfer of data (data retrieval) from ECS to TSDIS via the Data Request/DRA and DAN/DAA protocol.

Nominal transfers and error and exception handling are verified.

Test Configuration:

- Hardware: Ingest Server.
- Software: INGST, DCCI, INCI CSCIs.
- Test Tools: TSDIS simulators.

Test Data:

Test Data	File Name / Location
Dummy TRMM product data file for transmission from TSDIS to ECS.	ext02_level_0.dat
Dummy TRMM ancillary data file for transmission from TSDIS to ECS.	ext02_anc.dat
Dummy TRMM product data file for transmission from ECS to TSDIS	ext02_reproc.dat

Requirements Verified:

Mission Essential:
DADS0145 DADS0170 DADS0250 DADS1070 DADS1380 DADS1400
EOSD0500 EOSD0730 EOSD1607 EOSD1608 SDPS0020 SDPS0080

Mission Fulfillment:
EOSD5020

Procedures:

Test Set-up:

Step	Action	Expected Results	Comments
1.	Log in as DAAC operator		
2.	Open a UNIX script file to maintain test history Enter:**script** <**filename**>		
3.	Start up TSDIS simulation and verify ready to support test.		

Test Execution:

EXT02.1 Transfer of TRMM Data Products from TSDIS

Step	Action	Expected Results	Comments
1.	Logon to the DAAC Ingest Server and Gateway Server workstations. Enter:<**login id**> Enter:<**password**>		For in house testing the EDF DAAC Ingest and Gateway Servers and will act as the Ingest and Gateway Servers for all DAACs.
2.	Start the Gateway and Ingest Server processes if they are not currently running. You must **dce_login** prior to starting the Ingest Server process.		

Step	Action	Expected Results	Comments
3.	On the DAAC Ingest workstation set the "**DAA message option**" to "**Accepted**" and the "**DDN message option**" to "**Successful**".		
4.	Remote logon to the simulated Data Provider (TSDIS) workstation three times using three xterm's.		
5.	On the second xterm change directory to the TSDIS simulator executable directory and then start up the simulator user interface.		
6.	On the first xterm change directory to the TSDIS simulator executable directory and then start up the simulator.		
7.	On the third xterm window configure the correct authentication request file (valid) for the GSFC DAAC.		
8.	On the first xterm send a valid Authentication Request to the GSFC DAAC.	Successful transmission of Authentication Request.	
9.	On the second xterm, after receiving the Authentication Response send valid GDAN-2 to the GSFC DAAC.	Successful transmission of GDAN-2.	GDAN-2 contains VIRS L1A - 1B and Browse data.

Step	Action	Expected Results	Comments
10.	After the DAAC Ingest Server receives the DDA get a printout of the DDN, the DAA, and the Authentication Response using the third xterm and then delete all messages.	The Authentication Response should indicate that your Authentication Request was accepted. The DAA should indicate that GDAN-2 was accepted. The DDN should indicate that the data was transferred successfully.	Use the parser tool 'prtm' to get the Authentication Response, DAA and DDN in ASCII form.
11.	On the DAAC Ingest Server workstation, printout the Event Log.	The Event Log should contain entries for all of the ingest messages.	
12.	On the DAAC Ingest Server workstation, printout a listing of the temporary storage directory.	The listing of the temporary storage directory should contain all files identified in GDAN-2.	
13.	On the second xterm shutdown the simulator.		
14.	On the second xterm start up the simulator user interface.		
15.	On the first xterm start up the simulator.		
16.	On the third xterm window configure the correct authentication request file (valid) for the MSFC DAAC.		
17.	On the first xterm send a valid Authentication Request to the MSFC DAAC.	Successful transmission of Authentication Request.	
18.	On the second xterm, after receiving the Authentication Response send valid MDAN-5 to the MSFC DAAC.	Successful transmission of MDAN-5.	MDAN-5 contains (PR, TMI, GV) L1A - 3B, VIRS "combined" and Browse data

Step	Action	Expected Results	Comments
19.	After the DAAC Ingest Server receives the DDA get a printout of the DDN, the DAA, and the Authentication Response using the third xterm and then delete all messages.	The Authentication Response should indicate that your Authentication Request was accepted. The DAA should indicate that MDAN-5 was accepted. The DDN should indicate that the data was transferred successfully.	Use the parser tool 'prtm' to get the Authentication Response, DAA and DDN in ASCII form.
20.	On the DAAC Ingest Server workstation, printout the Event Log.	The Event Log should contain entries for all of the ingest messages.	
21.	On the DAAC Ingest Server workstation, printout a listing of the temporary storage directory.	The listing of the temporary storage directory should contain all files identified in MDAN-5.	
22.	On the second xterm shutdown the simulator.		
23.	On the DAAC Ingest workstation delete all files that may reside in the temporary storage directory. Enter: **rm -f /Ir1_IT/INGEST/temp_store/***		
24.	Logoff all xterm's and then logoff the DAAC Ingest and Gateway Server workstations.		

Post Test Analysis:

No post test analysis is necessary for this test.

EXT02.2 Nominal TRMM Data Transfer to TSDIS

Step	Action	Expected Results	Comments
1.	Logon to the EDF DAAC Data Server workstation. Enter:<**login id**> Enter:<**password**>		For in house testing the EDF DAAC Data Server will act as the Data Server for all DAACs.
2.	Start the Data Server and Gateway process(es) if they are not currently running.		
3.	Remote logon to the simulated Data Provider (TSDIS) workstation three times using three xterm's.		
4.	On the second xterm change directory to the simulator executable directory and then start up the simulator user interface. Enter: **cd/data/TSDIS/consumer** Enter: **ui**		
5.	On the first xterm change directory to the simulator executable directory and then start up the simulator. Enter: **cd /data/TSDIS/consumer** Enter: **sim**		
6.	On the third xterm window configure the correct Authentication Request file for the GSFC DAAC. Enter: **cd /data/TSDIS/consumer** Enter: **cp GSFC/valid_AR dsd_dsc_authent_netrc.txt**		

Step	Action	Expected Results	Comments
7.	On the first xterm send a valid Authentication Request to the GSFC DAAC. Enter: **n**	Successful transmission of Authentication Request.	
8.	After receiving the Authentication Response get a printout of it using the third xterm. Enter: **prtm %AUTH_RESP_001.mg** Enter: **y** Enter: **lp -d<printer> %AUTH_RESP_001. msg_prt**	The Authentication Response should indicate that your Authentication Request was accepted.	
9.	On the third xterm window configure a valid Data Request file for the GSFC DAAC. Enter: **cd /data/TSDIS/consumer/data** Enter:		
10.	On the first xterm send the valid Data Request to the GSFC DAAC. Enter: **n**	Successful transmission of Data Request.	
11.	After receiving the DAN get a printout of it using the third xterm. Enter:	The DAN should indicate that your Data Request was accepted and contain a pointer to the requested files.	
12.	On the second xterm shutdown the simulator. Enter: **10** Enter: **y**		
13.	On the second xterm start up the simulator user interface. Enter: **ui**		

Step	Action	Expected Results	Comments
14.	On the first xterm start up the simulator. Enter: **sim**		
15.	On the third xterm window configure the correct Authentication Request file for the MSFC DAAC. Enter: **cp MSFC/valid_ARdsd_dsc_authent_netrc.txt**		
16.	On the first xterm send a valid Authentication Request to the MSFC DAAC. Enter: **n**	Successful transmission of Authentication Request.	
17.	After receiving the Authentication Response get a printout of it using the third xterm. Enter: **prtm %AUTH_RESP_001.msg** Enter: **y** Enter: **lp -d<printer> %AUTH_RESP_001.msg_prt**	The Authentication Response should indicate that your Authentication Request was accepted.	
18.	On the third xterm window configure a valid Data Request file for the MSFC DAAC. Enter: **cd /data/TSDIS/Consumer/data**		
19.	On the first xterm send the valid Data Request to the MSFC DAAC. Enter: **n**	Successful transmission of Data Request.	

Step	Action	Expected Results	Comments
20.	After receiving the DAN get a printout of it using the third xterm. Enter:	The DAN should indicate that your Data Request was accepted and contain a pointer to the requested files.	
21.	On the second xterm shutdown the simulator. Enter: **10** Enter: **y**		
22.	Logoff all xterm's and then logoff the EDF DAAC Data Server workstation.		

Post Test Analysis:

No post test analysis is necessary for this test.

EXT02.3 Error and Exception Handling

Step	Action	Expected Results	Comments
1.	Logon to the EDF DAAC Data Server workstation. Enter:<login id> Enter:<password>		For in house testing the EDF DAAC Data Server will act as the Data Server for all DAACs.
2.	Start the Data Server process(es) if they are not currently running.		
3.	Remote logon to the simulated Data Provider (TSDIS) workstation three times using three xterm's.		
4.	On the second xterm change directory to the simulator executable directory and then start up the simulator user interface. Enter: **cd /data/TSDIS/consumer** Enter: **ui**		
5.	On the first xterm change		

Step	Action	Expected Results	Comments
	directory to the simulator executable directory and then start up the simulator. Enter: **cd /data/TSDIS/consumer** Enter: **sim**		
6.	On the third xterm window configure the correct Authentication Request file for the GSFC DAAC. Enter: **cd /data/TSDIS/consumer** Enter: **cp GSFC/valid_AR dsd_dsc_authent_netrc.txt**		
7.	On the first xterm send a valid Authentication Request to the GSFC DAAC. Enter: **n**		
8.	After receiving the Authentication Response get a printout of it using the third xterm. Enter: **prtm %AUTH_RESP_001.msg** Enter: **y** Enter: **lp -d<printer> %AUTH_RESP_001.msg_prt**		
9.	On the third xterm window configure an invalid Data Request file for the GSFC DAAC. Enter: **cd /data/TSDIS/consumer/data** Enter:		

Step	Action	Expected Results	Comments
10.	On the first xterm send the invalid Data Request to the GSFC DAAC. Enter:**n**	Successful transmission of Data Request.	
11.	After receiving the DAN get a printout of it using the third xterm. Enter:	The DAN should indicate that your Data Request was not accepted.	
12.	On the second xterm shutdown the simulator. Enter:**10** Enter:**y**		
13.	On the second xterm start up the simulator user interface. Enter:**ui**		
14.	On the first xterm start up the simulator. Enter:**sim**		
15.	On the third xterm window configure the correct Authentication Request file for the MSFC DAAC. Enter: **cp MSFC/valid_ARdsd_dsc_authent_netrc.txt**		
16.	On the first xterm send a valid Authentication	Successful transmission of Authentication Request.	

Step	Action	Expected Results	Comments
17.	After receiving the Authentication Response get a printout of it using the third xterm. Enter: **prtm %AUTH_RESP_001.msg** Enter: **y** Enter: **lp -d<printer> %AUTH_RESP_001.msg_prt**	The Authentication Response should indicate that your Authentication Request was accepted.	
18.	On the third xterm window configure an invalid Data Request file for the MSFC DAAC. Enter: **cd /data/TSDIS/Consumer/data** Enter:		
19.	On the first xterm send the invalid Data Request to the MSFC DAAC. Enter: **n**	Successful transmission of Data Request.	
20.	After receiving the DAN get a printout of it using the third xterm. Enter:	The DAN should indicate that your Data Request was not accepted.	
21.	On the second xterm shutdown the simulator. Enter: **10** Enter: **y**		
22.	Logoff all xterm's and then logoff the EDF DAAC Data Server workstation.		

Post Test Analysis:

No post test analysis is necessary for this test.

Test Termination:

Step	Action	Expected Results	Comments
1.	Print the test history log from the script file. Enter: **ctrl-D** to halt the script command. Print the MSS Event Log. Enter: **lpr-P** <printer name> <filename>	 Operator commands no longer logged. The history log is printed.	
2.	Take down the TSDIS simulator.		

4.4 EXT03 - NOAA and Non-EOS Ancillary Data Ingest

Test Objectives:

This test verifies the capability of ECS at the DAACs to receive and ingest Non-EOS and NOAA ancillary data sets from both NESDIS and DAO. Specific objectives to be tested are:

- Polling and retrieval of ancillary data.
- Validation and ingest of ancillary data products into the ECS data servers.
- Availability of ingested ancillary data for algorithms execution and other uses.

Test Configuration:

- Hardware: Ingest Server.
- Software: INGST, DCCI, INCI CSCIs.
- Test Tools: DAO and NESDIS simulation

Test Data:

Test Data	File Name / Location
NMC Ancillary Data FNL	
NESDIS Ancillary Data GPCP GPCC AVHRR-Aerosol AVHRR-Vegetation Index SSM/I-Snow/Ice Cover	

Requirements Verified:

Mission Essential:
DADS0250 DADS0260 EOSD0500 ESN-0290 SDPS0020 SDPS0080

Mission Fulfillment:
EOSD1710

Procedures:

Test Set-up:

Step	**Action**	**Expected Results**	**Comments**
1.	Log in as operator		
2.	Open a UNIX script file to maintain test history. Enter: **script**<**filename**>		

Test Execution:

EXT03.1 Polling and Transfer of NOAA and Non-EOS Ancillary Data

This test case addresses nominal and faulty transmissions of NOAA/Non-EOS ancillary data to ECS. The standard sequence to be executed involves the following steps:

Step	Action	Expected Results	Comments
1.	Logon to the EDF DAAC Ingest Server workstation. Enter:<**login id**> Enter:<**password**>		For in house testing the EDF DAAC Ingest Server will act as the Ingest Server for all DAACs.
2.	Remote logon to the simulated Data Provider (NESDIS) workstation using an xterm.		
3.	Set the POLL_TIMER variable to 30 seconds.		
4.	Start the Ingest Server Polling process without any of the arguments on the Ingest Server workstation..		
5.	After 1 minute print-out the Event log at the simulated	The Event log should contain a Polling Ingest entry stating that the environment variables have not been set.	
6.	Start the Ingest Server Polling process without the Delivery Record argument on the Ingest Server workstation.		
7.	After 1 minute print-out the Event log at the simulated LaRC DAAC.	The Event log should contain a Polling Ingest entry stating that the Delivery Record File Flag environment variable has not been set.	

Step	Action	Expected Results	Comments
8.	Start the Ingest Server Polling process without the Data Type argument on the Ingest Server workstation.		
9.	After 1 minute print-out the Event log at the simulated LaRC DAAC.	The Event log should contain a Polling Ingest entry stating that the Directory and Data Type environment variables have not been set.	
10.	Start the Ingest Server Polling process with all of the necessary arguments on the Ingest Server workstation.		
11.	After 2 minutes print-out the Event log at the simulated	The Event log should contain a Polling Ingest entry every 30 seconds.	
12.	Set the POLL_TIMER variable to 60 seconds.		
13.	After 4 minutes print-out the Event log at the simulated	LaRC DAAC.The Event log should contain a Polling Ingest entry every 60 seconds.	
14.	Set the POLL_TIMER variable to 600 seconds.		
15.	On the simulated NESDIS workstation place simulated TRMM ancillary data files in the LaRC DAAC Ingest directory.		Ancillary data files: anc_vin_11 anc_vin_12 anc_vin_13
16.	After 10 minutes print-out the Event log at the simulated LaRC DAAC.	The log should contain a Polling Ingest entry identifying the TRMM ancillary data files that were placed in the LaRC DAAC Ingest directory on the simulated NESDIS workstation.	
17.	Print-out the Polling Ingest comparison file	The file NOAA.Old should list the files that	NOAA.Old should list the following:

Step	Action	Expected Results	Comments
	NOAA.Old	were ingested.	anc_vin_11 anc_vin_12 anc_vin_13
18.	On the DAAC Ingest Server workstation, printout a listing of the temporary storage directory.	The directory listing should contain the data that were in the LaRC DAAC Ingest directory on the NESDIS workstation.	
19.	Use the UNIX data comparison tool "diff" to compare the data received at the simulated LaRC DAAC to the original data at the simulated NESDIS.	The comparison tool should return a successful comparison.	
20.	After 10 minutes print-out the Event log at the simulated LaRC DAAC.	The log should contain a Polling Ingest entry stating that no new TRMM ancillary data was placed in the LaRC DAAC Ingest directory on the simulated NESDIS workstation.	
21.	Print-out the Polling Ingest comparison file NOAA.Old	The file NOAA.Old should not have any new files listed.	NOAA.Old should list the following: anc_vin_11 anc_vin_12 anc_vin_13
22.	On the simulated NESDIS workstation place simulated TRMM ancillary data files in the LaRC DAAC Ingest directory.		Ancillary data files: anc_agaf_21 anc_agaf_22

Step	Action	Expected Results	Comments
23.	After 10 minutes print-out the Event log at the simulated LaRC DAAC.	The log should contain a Polling Ingest entry identifying the TRMM ancillary data that were placed in the LaRC DAAC Ingest directory on the simulated NESDIS workstation.	
24.	Print-out the Polling Ingest comparison file NOAA.Old	The file NOAA.Old should list the new files that were ingested along with the previous files that had been ingested.	NOAA.Old should list the following: anc_vin_11 anc_vin_12 anc_vin_13 anc_agaf_21 anc_agaf_22
25.	On the DAAC Ingest Server workstation, printout a listing of the temporary storage directory.	The directory listing should contain the data that were in the LaRC DAAC Ingest directory on the NESDIS workstation.	

Post Test Analysis:

No post test analysis is necessary for this test.

EXT03.2 NOAA Ancillary Data Availability for ECS Operations

This test case demonstrates the availability of the ingested NOAA ancillary data to ECS users. During Ir1 testing, data sets will reside in temporary storage.

Step	Action	Expected Results	Comments
1.	Log into the V0 system locally. Enter:<**login id**>. Enter:<**password**>		
2.	Perform a V0 search using the following criteria: (TBD)	The data sets located should include: **(**list - TBD)	
3.	Transfer the data set identified in step 2 to the staging area of PDPS.		
4.	Log into the V0 system		
5.	Perform a V0 search using the following criteria: (TBD)	The data sets located should include: (list - TBD)	
6.	Transfer data set from the remote DAAC to the local DAAC.	The selected data sets are transferred.	
7.	Verify completion of file transfer through UNIX directory listing with time stamps and file sizes.	File parameters in DAAC directory match those from the remote DAAC directory.	

Post Test Analysis:

No post test analysis is necessary for this test.

Test Termination:

Step	Action	Expected Results	Comments
1.	Log off the ECS.	Return to UNIX prompt.	
2.	Print history logs.		

4.5 INT01 - System Deployment Verification

Test Objectives:

The CAT INT01 is an inspection/analysis process to insure that ECS has been properly deployed at each DAAC and the SMC per Release Plan Specification and Version Description Document. This test will be performed at the end of January 1996 before the execution of the other tests begins. Specific test objectives are:

Verifying system protocols, policies and procedures, hardware, and software are under configuration management control and correspond to Ir1 Release specifications through the analysis of documentation.

Test Configuration:

Hardware: Site configuration.
Software: ClearCase, CM tool.
Test Tools: None.

Test Data:

None.

Requirements Verified:

Mission Essential:

EOSD0502	EOSD3200	ESN-1140	ESN-1340	ESN-1350	PGS-0490
PGS-1015	PGS-1020	PGS-1025	PGS-1030	SMC-2505	SMC-2510
SMC-2515	SMC-4305				

Mission Fulfillment:
None.

Procedures:

Test Set-up:

Step	Action	Expected Results	Comments
1.	Acquire a list from CM of all software delivered with the release.	A printing of a worksheet with S/W information.	Verify date of print out to be current.
2.	Acquire a list from CM of all hardware delivered with the release.	A printing of a worksheet with H/W information.	Verify date of print out to be current.
3.	Acquire a list of all policy and procedures associated with Ir1 from the EDF. The list should include dates of publication.	A printing of a worksheet with policy and procedure information.	Verify date of print out to be current.
4.	Acquire the Ir1 Installation Plan for the ECS Project (August 1995, 800-TP-001-001).	A list of the software and hardware configurations, and a bill of materials.	Use the most recent version available.
5.	Acquire the Release-B CSMS Release and Development Plan (October 1995, 307-CD-005-001 / 329-CD-005-001), which contains Ir1 information, and the SDPS Release and Development Plan for the ECS Project (March 1995, 307-CD-002-002, 329-CD-002-002)	A list of the Configuration Items (CIs) and S/W components of the Communications and System Management Subsystem (CSMS) of the ECS. A list of the Configuration Items (CIs) and S/W components of the Science Data Processing Segment (SDPS) of the ECS.	Use the most recent versions available.
6.	Acquire a list of all IRDs and ICDs associated with the Ir1 release.		
7.	Acquire a list of all policies and procedures associated with the Ir1 release.	Documentation describing the policies and procedures for each DAAC.	

Test Execution:

INT01.1 Site Hardware Configuration Verification

This test case demonstrates the verification of system hardware installed at the site. The configuration management tool is used to verify that the hardware is under control and corresponds to the release specification and/or version description document through analysis of those documents.

Step	Action	Expected Results	Comments
	There are no test execution steps for this test case. The test is performed entirely by inspection/analysis and is covered in the post-test analysis section below.		

Post Test Analysis:

Step	Action	Expected Results	Comment
Note:	Compare the information gathered in steps 2 and step 4 of the test set-up to insure the following:		
1.	1) That there is compatibility between the database worksheet and to the release specification and/or version description document	All Ir1 specified hardware is under CM.	

INT01.2 Site Software Configuration Verification

This test case demonstrates the verification of system software, software tools, databases, and libraries installed at the site. The configuration management tool is used to verify that the software is under control and corresponds to the release specification and/or version description document through analysis of those documents.

Step	Action	Expected Results	Comments
	There are no test execution steps for this test case. The test is performed entirely by inspection and is covered in the post test analysis section below.		

Post Test Analysis:

Step	Action	Expected Results	Comment
Note:	Compare the information gathered in steps 1 and steps 4 & 5 of the test set-up to insure the following:		
1.	1) That there is compatibility between the database worksheet and to the release specification and/or version description document	All Ir1 specified software is under CM.	

INT01.3 Protocol Verification

This test case verifies the protocols to be used by the ECS.

Step	Action	Expected Results	Comments
	There are no test execution steps for this test case. The test is performed entirely by inspection and is covered in the post test analysis section below.		

Post Test Analysis:

Step	Action	Expected Results	Comment
Note:	Compare the information gathered in steps 2 and in steps 4 & 6 of the test set-up to insure the following:		
1.	1) That there is compatibility between the physical devices and the corresponding medium access control (MAC) with ISO and ANSI standards.	The physical devices and the corresponding MAC are compatible with ISO and ANSI standards.	

Step	Action	Expected Results	Comment
2.	2) That TCP/IP communications protocols and services as required by external elements are supported.	That TCP/IP protocols and services are supported by each external element.	

INT01.4 Policy and Procedure Management

This test case verifies the availability and management of system policies and procedures at the DAACs.

Step	Action	Expected Results	Comments
	There are no test execution steps for this test case. The test is performed entirely by inspection and is covered in the post test analysis section below.		

Post Test Analysis:

Step	Action	Expected Results	Comment
Note:	Compare the information gathered in step 3 and 6 of the test set-up to insure the following:		
1.	1) That there is compatibility between the database worksheet and to the release specification and/or version description document	All Ir1 specified policies and procedures are maintained.	

Test Termination:

Step	Action	Expected Results	Comments
1.	Log off ECS system.	Return to UNIX prompt.	
2.	At UNIX prompt, print out history logs.		

4.6 SFT01 - Network Operations and Monitoring

Test Objectives:

This test verifies the network operations and administration at the SMC. Specific objectives of this test are:

- Access interfaces to display network configuration and status both locally and at the DAACs, through V0 WAN connectivity.
- Monitor and manage network performance through the use of thresholds and statistics.
- Evaluate network fault isolation and response mechanisms.

Test Configuration:

- Hardware: MSS Server, V0 LAN at each site, V0 WAN.
- Software: MCI, INCI CSCIs.
- Test Tools: None.

Test Data:

None.

Requirements Verified:

Mission Essential:

ESN-0010	ESN-0070	ESN-0210	ESN-0620	ESN-0640	ESN-0650
ESN-0740	ESN-0760	ESN-0775	ESN-0790	ESN-0800	ESN-0830
ESN-0840	ESN-0900	ESN-1060	ESN-1070	PGS-0430	

Mission Fulfillment:
None.

Procedures:

Test Set-up:

Step	Action	Expected Results	Comments
1.	Select a network threshold value to modify which can easily be exceeded to result in an out of limit event occurring. For example, **Disk%Util.**	Record network threshold name and recommended value: _____	
2.	Select large HDF and postscript files to be stored in sft01.2, step 18.		
3.	Start a UNIX script file to record test activities. Enter: **script** <filename>	Script file is started, record filename here: _____	

Test Execution:

SFT01.1 Network Configuration and Status Monitoring

This test case verifies the capability to view the network configuration and to assess the status of each of the components.

Step	Action	Expected Results	Comments
1.	Login to a DAAC MSS Server workstation (HP) in the EDF as an administrator. Enter:<**login id**> Enter:<**password**> Initialize HP OpenView. Enter: <**cd /usr/OV/bin/ovw** > Enter:< **ovw &** >	Access granted and network monitoring tool is displayed on the screen.	

Step	Action	Expected Results	Comments
2.	Generate a report summarizing the status of the local network devices in the present configuration. Select the output of the report to the console, a disk file, and a printer.	Report generated and all three outputs contain the same information.	
3.	Select to view the network routers. Starting from the top level map, traverse down the internet submaps to view the routers. Compare the information in the report with the display.	Display showing the status of the network routers appears on the screen. Information on the report verified.	Verify that all routers are functional.
4.	Select to view the network links. Starting from the top level map, traverse down the internet submaps to view the links. Compare the information in the report with the display.	Display showing the status of the network links appears on the screen. Information on the report verified.	Verify that all links are functional.
5.	Select to view the network gateways. Starting from the top level map, traverse down the internet submaps to view the gateways. Compare the information in the report with the display.	Display showing the status of the network gateways appears on the screen. Information on the report verified.	Verify that all gateways are functional.

Step	Action	Expected Results	Comments
6.	Select to view statistics detailing network configuration and status. Compare the information in the report with the display.	Display showing network configuration and status statistics appears on the screen. Information on the report verified.	
7.	Close all windows and exit OpenView. End Test.		

Post Test Analysis:

No post test analysis is necessary for this test.

SFT01.2 Network Performance Monitoring

This test case verifies the monitoring of network performance through the use of network thresholds.

Step	Action	Expected Results	Comments
1.	Login to a DAAC MSS Server workstation (HP) in the EDF as an administrator. Enter:<**login id**> Enter:<**password**>	'Enter Password' will be displayed 'host name {user name}' will be displayed	
2.	Initialize the HP OpenView application: Enter: <**cd /usr/OV/bin/ovw** > Enter: <**ovw &**>	Overall network topology is accurately displayed.	
3.	Double click the "**EDF**" icon.	Map depicting EDF configuration is accurately displayed.	
4.	From the "**options**" pull down menu select "**Data & Thresholds: SNMP...**"	A MIB Data Collection window is observed.	

Step	Action	Expected Results	Comments
5.	From the "**MIB Data Collection**" window select a performance metric, such as "**Disk%Util**"	From the collection summary box within the MIB Data Collection window verify that the PMAS provides a configurable number of thresholds for each performance metric	
6.	From the "**MIB Object Collection summary box**" within the MIB Data collection window select the "**MIB object**".	Collection Data box is highlighted.	
7.	Enter "**Threshold and Rearm values**" in the collection details box and click on Replace button.	The new values will appear in the MIB object collection summary box.	***Note:*** In order to find out what will be the proper values for the Threshold and Rearm, click on the show data button from the MIB Data Collection window and base on the current value column to determine what will be the proper value for test.
8.	Reselect the "**MIB Object**" from the "**MIB Object collection Details**" box.		
9.	Configure the threshold event by clicking on the "**Configure Threshold Event**" button.	Event configuration window will be observed.	
10.	Select the "**Event Name**" which has the same event number as the trap number defined in the "**Collection Details**" box for the threshold event.		
11.	Click on the "**modify**" button.	The modify event window will be observed.	
12.	Configure the pop up notification field to display a		

Step	Action	Expected Results	Comments
	message to the console when the threshold event is exceeded.		
13.	Click on the "**OK**" button.	The modify event window will disappear.	
14.	Select the "**event name**" which has the event number as the trap number +1 in the "**Collection Details**" box for the rearm event.		
15.	Configure the "**Popup notification**" field to display a message to the console when the rearm event is met.		
16.	Click on the "**OK**" button.	The modify event window will disappear.	
17.	Click on the "**Apply**" or "**OK**" button from the event configuration window to replace the old information with the updated information.		
18.	Exceed the limit in step 7 by storing as many large postscript and HDF files to the system storage device as possible without damaging any existing files on the system.	Verify that when the threshold is exceeded, the popup window is displayed.	
19.	Remove the files that were stored in step 18 to bring the hard disk storage capacity below the rearm level.	Verify that when the rearm value is met, the popup window is displayed.	
20.	Generate a report showing the network's performance.	Threshold value exceeded should appear on the report.	

Step	Action	Expected Results	Comments
21.	Generate a short and long term trend analysis report.	The report should contain the following information: a. Operational status b. Performance of all resources. c. Maintenance activities.	
22.	Close all windows and exit OpenView. End test.		

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Verify that the history log captured the events during the test.	All events should be recorded in sequence.	

SFT01.3 Network Fault Isolation and Recovery

This test case demonstrates the capability to detect faults within the network.

Step	Action	Expected Results	Comments
1.	Login to a DAAC MSS Server workstation (HP) in the EDF as an administrator. Enter:<**login id**> Enter:<**password**>	'Enter Password' will be displayed 'host name {user name}' will be displayed	
2.	Initialize the HP OpenView application: Enter: <**cd /usr/OV/bin/ovw** > Enter:<**ovw &**>	HP OpenView will initialize.	
3.	Double click on the "**EDF**" icon to bring up the EDF window.	Map depicting the EDF configuration is accurately displayed.	
4.	Select "**Options**" from the menu bar, followed by "**topology/status polling: IP**"	The topology/status polling window is displayed.	

Step	Action	Expected Results	Comments
5.	Configure the polling interval: click the "**polling master switch**", and "**configuration checking switch**" buttons and putting "**1s**" in the "**configuration polling interval**" box.	The polling interval is set to one second.	
6.	Select "**Diagnose**" from the menu bar, followed by "**network connectivity**", followed by "**ping**"	A ping window is displayed.	
7.	Enter the new IP address in the "**To name or IP address**" box.	Data is displayed that is similar to the following: <64 bytes from 192.150.28.112:icmp_seq = 247, time=6 ms.	
8.	Click on the "**stop**" button.		
9.	Click on the "**close**" button.		
10.	Disconnect a hardware device(i.e., computer, printer) from the network.	The symbol of the device that was disconnected will turn red and the EDF icon in the Ir1 map will turn yellow.	
11.	Double click on the "**red device symbol**".	Node submap opens with one of the interfaces red.	
12.	Reconnect the hardware device.	The maps will return to their original state.	
13.	Click on the "**all events**" box in the "**Event Categories**" window.	The "all events browser" window is displayed.	
14.	Examine the event log to determine whether all appropriate events have been documented.		
15.	Select "**File**" from the menu bar, followed by "**close**".		
16.	Double click on the "**GSFC DAAC icon**".	The GSFC submap appears.	

Step	Action	Expected Results	Comments
17.	Click on one of the symbols (devices) in this submap.	The symbol becomes highlighted.	
18.	Select "**Misc**" from the menu bar, followed by "**terminal connect**", followed by "**IP/TCP/SNMP**..."	The test all protocols window is displayed with the following information: ICMP Echo < 10ms; TCP connect = ok and SNMP Get=ok.	
20.	Click on the "**close**" button.		
21.	Select "**diagnose**" from the menu bar, followed by "**network connectivity**". followed by "**demand poll**".	A demand poll window is displayed with a list of the poll results.	
22.	Click on the "**close**" button.		
23.	Select "**diagnose**" from the menu bar, followed by "**network connectivity**", followed by "ping".	A ping window is displayed with data similar to the following <64 bytes from 128.183.118.44: icmp_seq=247, time =6ms.	
24.	Click on the "**stop**" button.		
25.	Click on the "**close**" button.		
26.	Select "**monitor**" from the menu bar, followed by "**network configuration**", followed by "services".	A services window is displayed with a listing of all of the available services.	
27.	Click on the "**close**" button.		
28.	Select "**ECS**" from the menu bar, followed by "display current reports".	A list of possible reports are displayed.	
29.	Select a report such as "**traffic reports**".	The OpenView grapher window is displayed.	
30.	Select "**File**" from the menu bar, followed by	The print OpenView Grapher window is	

Step	Action	Expected Results	Comments
	"print...".	displayed.	
31.	Click on the "**Apply**" button.	The graph prints out.	
32.	Click on the "**Cancel**" button.		
33.	Select "**File**" from the menu bar, followed by "**save as**..."	The save data window is displayed.	
34.	Click on the "**Apply**" button.	The graph is saved to disk.	
35.	Click on the "**Cancel**"button.		
36.	Select "**File**" from the menu bar, followed by "**Exit**" to close the "**grapher window**".		
37.	Repeat the previous step until you close all the reports.		
38.	Select "**options**" from the menu bar, followed by "**data collection & thresholds:SNMP**"	The MIB data collection window appears.	
39.	Select "**ComputerSystem Users**" from the "**MIB objects"** configured for collection" window.		
40.	Select "**mss1hpedf.gsfc.nasa.gov**" from the "**MIB object collection summary**" window.		
41.	Change the values in the "**threshold**" and "**rearm**" boxes to two greater than the number of users currently on the system.		
42.	Click on the "**configure threshold event**..." button.	The event configuration window appears.	

Step	Action	Expected Results	Comments
43.	Click on "**Toomanyusers**" event and click on the "**modify**" button.	The modify event window appears.	
44.	Enter the following line in the "**Command for Automatic Action**" box: "**echo "Too many users on $2" |/usr/bin/mailx -s "Many users" <userid>@<mail ip address**>'. if it is not there yet		
45.	Enter the following line in the "**Popup Notification**" box: "**Number of Users Exceeded x**",		
46.	Click on the "**OK**" buttons.		
47.	In the window that you started OpenView from, start up two more login sessions.	A notify box should appear stating 'Number of Users Exceeded x'.	
48.	Enter:< **mailx**> on one of the workstation command line	Mail utility will start up.	
49.	Enter:<**n**> (until all messages are read)	There should be a new message that states: 'Too many users '.	
50.	Click on the "**printer icon**" and make sure the printer is 'online'.		
51.	Select "**Monitor**" from the menu bar, followed by "**MIB Values**", followed by "**Browse MIB: SNMP**...".	The 'Browse MIB' window is displayed.	
52.	Select "**private**" then click the ' Down Tree '		
53.	Select "**enterprises**" then click the "**Down Tree**"		
54.	Select "**hp**" then click the		

Step	Action	Expected Results	Comments
	"**Down Tree**".		
55.	Select "**nm**" then click the "**Down Tree**"		
56.	Select "**System**" then click the "**Down Tree**"		
57.	Select "**net-peripheral"** then click the "**Down Tree**"		
58.	Select "**net-printer**". then click the "**Down Tree**"		
59.	Select "**GeneralDeviceStatus**". Then click the "**Down Tree**"		
60.	Select "**gdStatusDisplay**"		
61.	Click on the "**Start Query**" button	'online' is displayed in the 'MIB Values' window.	
62.	Take the printer offline.		
63.	Click on the "**Start Query**" button	'offline' is displayed in the 'MIB Values' window.	
64.	Put the printer in test mode.		
65.	Click on the "**Start Query**" button	'test mode' is displayed in the 'MIB Values' window.	
66.	Click on the "**Close**" button		
67.	Close all windows and exit from OpenView. End test		

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Verify that the history log captured the events during the test.	All events should be recorded in sequence.	

Test Termination:

Step	Action	Expected Results	Comments
1.	Log off the both local and remote ECS sessions.	Return to UNIX prompt.	
2.	Enter: **ctrl-D** to halt the script command.	Operator commands no longer logged.	
3.	Enter: **lpr-P** <printer name> <filename>	The history log is printed.	

4.7 SFT02- System Operations and Administration

Test Objectives:

This test addresses the operation and administration of system hardware and software, including performance monitoring. Specific objectives of this test are:

- Monitor the status of non-communication related hardware and software.
- Monitor system performance through the management of performance thresholds.
- Evaluate system fault isolation and response mechanisms.
- Evaluate configuration management of procedures and policies.

Test Configuration:

- Hardware: MSS Server.
- Software: MCI, INCI, DCCI CSCIs.
- Test Tools: None.

Test Data:

None.

Requirements Verified:

Mission Essential:

EOSD0510	ESN-0650	ESN-0910	PGS0370	SMC-3300	SMC-3305
SMC-3370	SMC-3375	SMC-3380	SMC-3390	SMC-3395	SMC-3415
SMC-4310	SMC-4311	SMC-4315	SMC-4320	SMC-4325	SMC-8840

Mission Fulfillment:
EOSD0780

Procedures:

Test Set-up:

Step	**Action**	**Expected Results**	**Comments**
1.	Obtain a list of software applications that are monitored by the HP OpenView tool.	List generated.	
2.	Obtain a list of system thresholds (performance metrics) being monitored by HP OpenView.	List generated.	
3.	Start a UNIX script file to record test activities. Enter: **script** <filename>	Script file is started, record filename here: _____	

Test Execution:

SFT02.1 System Hardware Status Monitoring

This test case verifies the system capability to monitor both local and remote hardware within the DCE cell. This test is performed only on hardware associated with the ECS.

Step	Action	Expected Results	Comments
1.	Login to a DAAC MSS Server workstation (HP) in the EDF as an administrator. Enter:<**login id**>	' Enter Password ' will be displayed	
2.	Enter:<**password**>	'host name {user name}' will be displayed	
3.	Initialize HP OpenView Enter: <**cd /usr/OV/bin/ovw** > then Enter:<**ovw &**>	HP OpenView will initialize	
4.	To simulate a hardware failure disconnect the hardware component from the network. (i.e. printer)	EDF ICON turns yellow	
5.	Double-click on the "**yellow Internet symbol**".	EDF submap appears	
6.	A network submap opens and display the various segments connected to it.		
7.	If a red symbol is not visible double click "**on the yellow/blue**" until a red symbol appears	If symbol is red fault is isolated.	
8.	Double click on the "**red workstation symbol**". Node submap opens indication with one of the interfaces Red. The fault have been isolated to a single node.		
9.	Close all windows and exit OpenView. End of test.		

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Verify that the history log captured the events during the test.	All events should be recorded in sequence.	

SFT02.2 System Software Status Monitoring

This test case verifies the monitoring of system software. The system provides the capability to view software currently operating within the systems and their current status. This test is performed on software provided with ECS.

Step	Action	Expected Results	Comments
1.	Login to a DAAC MSS Server workstation (HP) in the EDF as an administrator. Enter:<**login id**> Enter:<**password**>	'Enter Password' will be displayed 'host name {user name}' will be displayed	
2.	Initialize Hp Openview by using the command Enter:<**cd /usr/OV/bin**> Enter:<**ovw &**>	To start the Hp OpenView graphical interface. A map is displayed showing the various DAACS.	
3.	Double click on the Icon for the "**EDF DAAC**"	A submap is displayed	
4.	Using a different Hpterm logon to Nickalus using appropriate password and ID as an administrator	Able to enter password and ID	
5.	Enter: <**/usr/mssdata/MSS/bin**> on Nickalus and Enter: <**testd &** >	To start the software application process.	
6.	Wait one minute and then kill the software application process Enter:< **Kill -9 'PID #'**>.	After a period of approx. 2 minutes the Nickalus Icon in the submap turns blue	
7.	Double click on the "**Nickalus icon**" .	A submap shall appear	
8.	Verify that the "**testd**	Testd Icon is red.	

Step	Action	Expected Results	Comments
	Icon" is red.		
9.	Observe a "**Process Down**" event popup window for the problem appears.	Popup widow listing problem appears.	Verify a Process Down event popup window for the problem appears.
10.	Restart the testd application process by Entering:<**testd &>** and verify the ICON turns back to green.	Testd Icon turns green.	
11.	Close all windows and exit OpenView. End test.		

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Verify that the history log captured the events during the test.	All events should be recorded in sequence.	

SFT02.3 System Performance Management

This test verifies the monitoring of system performance through the use of system thresholds.

Step	Action	Expected Results	Comments
1.	Enter: <**login id** > to login to a DAAC workstation in the EDF.	'Enter Password: will be displayed	
2.	Enter:<**password**>	'host name {user name}' will be displayed	
3.	Initialize HP OpenView by using the command Enter:< **cd /usr/OV/bin**> and Enter: <**ovw &** >	Hp Openview initializes	
4.	Double click on the "**EDF icon**".	A submap consisting of the manage objects appear	
5.	Click on one of the objects in the submap.	Object is highlighted.	

Step	Action	Expected Results	Comments
6.	Select from the "**OVW**" menu bar " **Monitor -> MIB Values -> Browse MIB:SNMP**" (Note: Click on the Down Tree button in order to go to the next level.)	The Browse MIB window appears.	
7.	In the Mib window browser click on **" mgmt->mib-2- >system->sysDescr"**	sysDescr shall be highlighted	
8.	Click on the **"Start Query"** button.	Definition/description of the object	
9.	Double click on the next object in the submap.	Next object is highlighted.	
10.	Click on the **" Reselect and the Start Query buttons"** in the order given.	A definition /description of the object is given	
11.	Repeat steps 9 and 10 for the remaining objects in the submap.		
12.	Select **"Options -> Data Collection & Threshold :SNMP -> Selected objects"**.	Mib Data Collection window appears	
13.	In the "**MIB DATA Collection window**" verify that they are a number of MIB objects configured for Collection.	Display of performance metrics in the MIB Object ID column	
14.	Click on **"Diskutil"** .	Performance metrics is highlighted.	
15.	In the "**MIB Object Collection Summary window"** click on the **"ADD"** button.	MIB Data Collection/Add collection for Disk % util window appears	

Step	Action	Expected Results	Comments
16.	In the "**MIB Data Collection window**" enter of the sources from the EDF submap and click on the "**Add**" button.	The 'Source selected. hitc.com' appears in the list of collection services box.	
17.	Click on **"OK".**	The selected object is added to the MIB Object collection summary.	
18.	Click on the object added in the "**MIB Object Collection summary window**" . Double click on the **"Show Data"** button in the "**MIB Objects Configured for Collection window**".	A window displaying the results of each polling interval of the object appears.	
19.	Double click on **"Graph -> View -> Statistics"**	The following statistics for the configurable period is given: Minimum, Average, Maximum, last value.	
20.	Select from the "**OVW**" menu bar "**Monitor -> MIB Values -> Browse MIB:SNMP**" (Note: Click on the Down Tree button in order to go to the next level.)	The Browse MIB window appears.	
21.	Using the MIB Browser click on the following in the sequence given: **"mgmt-> MIB-2 -> interfaces -> if table -> if entry**" (Note: click on the down tree button to go to the next level).	A list of network component are displayed. Such as operational status, type, speed, octets in/out, packets in/out, Discards in/out and errors in out.	

Step	Action	Expected Results	Comments
22.	Using the **" Start Query and the Deselect button"** verify that data can be retrieved from each interface component listed in step 21.	Data in Mib values box.	
23.	Close all open windows except the Ir1 map and its EDF submap.		
24.	Click on **"Misc -> Display current reports".**	Openview grapher window is displayed.	
25.	Close the OpenView graph.	Another grapher window is displayed.	
26.	Repeat step 25 until all collecting/performance/errors reports are completed. To close the window click on "**File**" and "**Exit**"		
27.	To print the reports select **"MISC -> Print current reports"**	Reports are printed to the printer.	
28.	All reports are logged to a postscript file. To view the report change directory to "**/user/msdata/MSS/report/ ' month_year of the report"** Enter: <**ls**> to list the various report. Enter: **<pg> <reportname>** to view the contents of the report. Depress : **"Enter key"** to view additional pages.		

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Examine the history log.	All changes to system thresholds should appear in the history log. Also, all requests for reports and the events performed to exceed threshold values should be recorded.	
2.	Examine performance report.	Verify that the threshold values which were exceeded appear in the report. The report should include operational status.	
3.	Examine resource utilization report.	Verify that the affected resources are marked in the report. The report should include maintenance activities performed on the resources.	

SFT02.4 Fault Isolation and Response

This test case is used as the all site test and demonstrates the capability to detect faults within the system. It also determines if the correct responses are generated.

Step	Action	Expected Results	Comments
1.	Enter:<**login id >** to login to a DAAC workstation in the EDF.	'Enter Password: will be displayed	
2.	Enter: <**password**>	'host name{user name}' will be displayed	
3.	Initialize HP OpenView by using the command Enter: < **cd /usr/OV/bin**> Enter: <**ovw &** >	Hp Openview initializes	
2.	Perform the steps necessary to exceed one of the system thresholds at the GSFC DAAC.	Display updates to show the exceeded threshold and recommends what actions are necessary to correct the problem.	
3.	Disable a hardware device at the LaRC DAAC.	Display updates to show the hardware device is not available and recommends what actions are necessary to correct the problem.	
4.	Simulate a stalled print queue at the EDC DAAC.	The display updates to show the stalled print queue and recommends what actions are necessary to correct the problem.	
5.	Stop one of the executing software programs at the MSFC DAAC.	The display updates to show the program is no longer running and recommends what actions are necessary to correct the problem.	
6.	Perform fault diagnosis testing.	The test should report the errors induced in steps 2 - 5.	

Step	Action	Expected Results	Comments
7.	Return the hardware device used in step 4 to its original state.	Display updates to show the device is on-line.	
8.	Return the print queue to its active state.	Display updates to show that the print queue is normal.	
9.	Restart the stopped software application.	Display updates to show the program is available once again.	

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Verify the history log.	The history log should contain all events performed in this test.	
2.	Verify the recommended actions to correct the problems detected.	The recommended solutions should be appropriate to the situation encountered.	

Test Termination:

Step	Action	Expected Results	Comments
1.	Log off the both local and remote ECS sessions.	Return to UNIX prompt.	
2.	Enter: **ctrl-D** to halt the script command.	Operator commands no longer logged.	
3.	Enter: **lpr-P** <printer name> <filename>	The history log is printed.	

4.8 SFT03 - System Access & Connectivity

Test Objectives:

This test verifies the capability of ECS to access the Version 0 (V0) LAN and WAN and use its capabilities. Specific objectives to be tested are:

V0 LAN and WAN access.
Protocol verification.
File and electronic message transfer.

Test Configuration:

Hardware: V0 LAN at each site, V0 WAN access, MSS server, printer (local and remote).
Software: DCCI, INCI, MCI CSCIs.
Test Tools: None.

Test Data:

Printable ASCII file at local and remote site.
User accounts and passwords at local and remote sites.
Binary and data files to be used for file transmissions.

Requirements Verified:

Mission Essential:

EOSD0500	EOSD0730	ESN-0003	ESN-0010	ESN-0070	ESN-0280
ESN-0290	ESN-0370	ESN-1140	ESN-1170	ESN-1180	

Mission Fulfillment:
None.

Procedures:

Test Set-up:

Step	Action	Expected Results	Comments
1.	Acquire a valid account name and password for the ECS.	Account / Password combination received.	
2.	Acquire the name of an ASCII file to be printed on a local printer.	Record local file name/path: _____	
3.	Acquire the name of a file to be printed on the remote printer.	Record remote file name/path: _____	
4.	Acquire two binary files to be used for file transmission: a. Binary unstructured b. Binary sequential.	Record binary file names/path: Unstructured: _____ Sequential _____	

Step	Action	Expected Results	Comments
5.	Acquire two text files to be used for file transmission: a. Unstructured text b. Sequential text.	Record text file names/path: Unstructured: _____ Sequential _____	
6.	Acquire a data file to be used for file transmission.	Record data file name/path: _____	
7.	Start a UNIX script file to record test activities. Enter: **script** <filename>	Script file is started, record filename here: _____	

Test Execution:

SFT03.1 LAN Access

This test case verifies access to the LAN.

Step	Action	Expected Results	Comments
1.	Attempt to log on to the ECS using a valid account with an invalid password.	System does not allow access.	
2.	Attempt to log onto the ECS using a valid account and password.	System allows access.	
3.	Enter: **SoftWindows** to bring up Microsoft Windows.	Display shows Microsoft Windows and Microsoft Office suite of programs.	
4.	Select the Microsoft Word option.	Microsoft Word window appears.	
5.	Open the file recorder in the Test Set-up step 2.	File is opened.	
6.	Enter: **cntrl P** to print the document.	Document is printed on the Ir1 laser printer.	

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Compare printed file against original file.	Files should be the same.	

SFT03.2 WAN Access

This test case verifies access to the WAN.

Step	Action	Expected Results	Comments
1.	Attempt to log onto a remote host using a valid account with an invalid password.	System does not allow access.	
2.	Attempt to log onto a remote host using a valid account and password.	System allows access.	
3.	Enter: **SoftWindows** to bring up Microsoft Windows.	Display shows Microsoft Windows and Microsoft Office suite of programs.	
4.	Select the Microsoft Word option.	Microsoft Word window appears.	
5.	Open the file recorder in the Test Set-up step 3.	File is opened.	
6.	Enter: **cntrl P** to print the document.	Document is printed on the Ir1 laser printer.	

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Compare printed file against original file.	The files should be identical.	

SFT03.3 File Transfer

This test case verifies SMC to DAAC transfer of files, via ftp and rcp and DAAC to SMC transfer of files, via ftp and rcp.

Step	Action	Expected Results	Comments
1.	Logon to the SMC workstation.	Access allowed.	
2.	Logon to a remote ECS host (GSFC, LaRC, EDC, or MSFC). Use the site under test. When testing the SMC, use any site.	Access allowed. Record site used: _____	
3.	At the SMC workstation enter: **cd <directory>** where directory is the path of the files in test set-up step 5.	Working directory set.	
4.	Enter: **ls -al**	Displays a list of files in the directory.	
5.	Enter: **ftp**	'ftp>' is displayed.	
6.	Enter: **open**	'(to)' is displayed.	
7.	Enter: <site ip address of site used in step 2>	'Name (host name: user name):' is displayed.	
8.	Enter: <username>	'Password:' is displayed.	
9.	Enter: <password>	'User <username> logged in ftp>' is displayed	
10.	Enter: **cd /**<directory name> where directory name is the name of the directory where the file is to be transferred to.	'CWD command successful' is displayed.	
11.	Enter: **ASCII**	Type set to 'A' is displayed.	
12.	Enter: **mput** <filenames> where filenames are the names of the unstructured and sequential text files listed in test set-up step 5.	Both files are transferred successfully.	

Step	Action	Expected Results	Comments
13.	At the remote site enter: **cd /**<directory> where directory is the same as that entered in step 10.	The directory is changed at the remote site.	
14.	At the remote site enter: **ls -al** and verify that the file transferred and that the size and checksum for both files are identical.	Information about files at the SMC and the remote site are the identical.	
15.	At the SMC enter: **binary**	Type set to 'I' is displayed.	
16.	Enter: **mput** <filenames> where filenames are the names of the binary structured and sequential files listed in test set-up step 4.	Both files are transferred successfully.	
17.	At the remote site enter: **cd /**<directory> where directory is the same as that entered in step 10.	The directory is changed at the remote site.	
18.	At the remote site enter: **ls -al** and verify that the file transferred and that the size and checksum for both files are identical.	Information about files at the SMC and the remote site are identical.	
19.	At the local site enter: **quit**	This command exits the ftp program. Return to UNIX prompt.	
20.	At the local site enter: **rcp** <data file name> <remote site name:path> where data file name is from the test set up step 6, remote site is the site logon to in step 2 and path is the directory to place the file.	The data file is transferred to the remote site.	

Step	Action	Expected Results	Comments
21.	At the remote site enter: **ls -al** and verify that the file transferred and the size and checksum for the files are identical.	Information about files at the SMC and the remote site are identical.	
22.	At the local site remove the files from the directory using the following command: **rm** <filename>	Files are deleted from the directory.	
23.	At the local site enter the command: **ls -al**	Verify that the files were deleted.	
24.	At the remote site workstation enter: **cd <directory>** where directory is the path of the files in test set-up step 5.	Working directory set.	
25.	Enter: **ls -al**	Displays a list of files in the directory.	
26.	Enter: **ftp**	'ftp>' is displayed.	
27.	Enter: **open**	'(to)' is displayed.	
28.	Enter: <site ip address of the SMC>	'Name (host name: user name):' is displayed.	
29.	Enter: <username>	'Password:' is displayed.	
30.	Enter: <password>	'User <username> logged in ftp>' is displayed	
31.	Enter: **cd /**<directory name> where directory name is the name of the directory where the file is to be transferred to at the SMC.	'CWD command successful' is displayed.	
32.	Enter: **ASCII**	Type set to 'A' is displayed.	
33.	Enter: **mput** <filenames> where filenames are the names of the unstructured and sequential text files listed in test set-up step 5.	Both files are transferred successfully.	

Step	Action	Expected Results	Comments
34.	At the remote site enter: **cd /**<directory> where directory is the same as that entered in step 31.	The directory is changed at the remote site.	
35.	At the SMC enter: **ls -al** and verify that the file transferred and that the size and checksum for both files are identical.	Information about files at the SMC and the remote site are identical.	
36.	At the remote site enter: **binary**	Type set to 'I' is displayed.	
37.	Enter: **mput** <filenames> where filenames are the names of the binary structured and sequential files listed in test set-up step 4.	Both files are transferred successfully.	
38.	At the SMC enter: **cd** /<directory> where directory is the same as that entered in step 31.	The directory is changed at the remote site.	
39.	At the SMC enter: **ls -al** and verify that the file transferred and that the size and checksum for both files are identical.	Information about files at the SMC and the remote site are identical.	
40.	At the remote site enter: **quit**	This command exits the ftp program. Return to UNIX prompt.	
41.	At the remote site enter: **rcp** <data file name> <SMC site name:path> where data file name is from the test set up step 6, remote site is the SMC and path is the directory to place the file.	The data file is transferred to the remote site.	
42.	At the SMC enter: **ls -al** and verify that the file transferred and size / checksum are identical.	Information about files at the SMC and the remote site are identical.	

Post Test Analysis:

No post test analysis is necessary for this test.

SFT03.4 Electronic Messages

This test case verifies DAAC to DAAC transfer of electronic messages. The EDF is also included in this test.

Step	Action	Expected Results	Comments
1.	Log onto the workstation at the site under test.	Access granted.	
2.	Enter: **mail** <userid at EDF@internet mail address> and hit enter key.	Enter the mail system and wait for the message text to be entered.	
3.	Type the message text to send to the EDF.	The message is displayed on the screen as it is entered.	
4.	Enter: **"."** to send the message to the EDF.	'host name (user name):' is displayed.	
5.	Enter: **mail** <userid at GSFC@internet mail address> and hit enter key.	The mail system waits for the message text to be entered.	
6.	Type the message text to send to the GSFC DAAC.	The message is displayed on the screen as it is entered.	
7.	Enter: **"."** to send the message to the GSFC DAAC.	'host name (user name):' is displayed.	
8.	Enter: **mail** <userid at LaRC@internet mail address> and hit enter key.	The mail system waits for the message text to be entered.	
9.	Enter the message text to send to the LaRC DAAC.	The message is displayed on the screen as it is entered.	
10.	Enter: **"."** to send the message to the LaRC DAAC.	'host name (user name):' is displayed.	
11.	Enter: **mail** <userid at EDC@internet mail address> and hit enter key.	The mail system waits for the message text to be entered.	

Step	Action	Expected Results	Comments
12.	Enter the message text to send to the EDC DAAC.	The message is displayed on the screen as it is entered.	
13.	Enter: **"."** to send the message to the EDC DAAC.	'host name (user name):' is displayed.	
14.	Enter: **mail** <userid at MSFC@internet mail address> and hit enter key.	The mail system waits for the message text to be entered.	
15.	Enter the message text to send to the MSFC DAAC.	The message is displayed on the screen as it is entered.	
16.	Enter: **"."** to send the message to the MSFC DAAC.	"host name (user name):' is displayed.	
17.	Enter: **q** to exit the mail system.	The system exits the mail system.	

Post Test Analysis:

The mail messages will be read and verified when test SFT05.2 is executed at each site.

Test Termination:

Step	Action	Expected Results	Comments
1.	Log off the both local and remote ECS sessions.	Return to UNIX prompt.	
2.	Enter: **ctrl-D** to halt the script command.	Operator commands no longer logged.	
3.	Enter: **lpr -P** <printer name> <filename>	The history log is printed.	

4.9 SFT04 - System Security Administration

Test Objectives:

This test verifies the system capability to define various levels of users and authenticate the associated privileges. Specific objectives to be tested are:

- Manage users through the use of the security registry.
- Specify and implement user groups.
- Authenticate and enforce user privileges and access.

Test Configuration:

- Hardware: MSS Server.
- Software: DCCI, INCI CSCIs.
- Test Tools: none.

Test Data:

None.

Requirements Verified:

Mission Essential:
ESN-0010 ESN-0650 SMC-5320 SMC-5325 SMC-5330 SMC-5335 SMC-5365 SMC-8880

Mission Fulfillment:
None.

Procedures:

Test Set-up:

Step	Action	Expected Results	Comments
1.	Acquire account name/password with privileges to modify the user account registry.		
2.	Start a UNIX script file to record test activities. Enter: **script** <filename>	Script file is started, record filename here: _____	

Test Execution:

SFT04.1 User Account Management

This test case addresses the management of DCE user accounts through the security registry. For Ir1, the DCE Host is at the EDF. When this test is run at a site other than the SMC, the operator must remotely log into the EDF to perform this test. The DCE accounts being added must already have valid UNIX user IDs.

Step	Action	Expected Results	Comments
1.	Log on to the Ir1 DCE Host in the EDF as a DCE cell administrator. Enter: **telnet dceserver** - or - **rsh dceserver**	Access to system granted.	
2.	Enter: **ypcat passwd | grep userid**	Search the password file for the four users names and UNIX id numbers.	This information is needed when creating the DCE user accounts. The id numbers are in the third column
3.	Enter: **dce_login_cell_admin**	Logs in to DCE as cell administrator.	
4.	Enter: **<admin_password>**	Password accepted.	
5.	Enter: **rgy_edit**	Brings up the DCE registry edit tool.	
6.	Enter: **do p**	Changes to principal domain to enter a new user.	
7.	Enter: **add**	Adds a new principle name.	
8.	Enter: <**user_idA**>	Enter user id of new user.	
9.	Enter: <**unix_ID_number**>	This is the number retrieved from the passwd file in step 2.	
10.	Enter full name of user.	Associates the user's full name to the user id.	
11.	Enter: **<return>**	Use default value for object creation quota.	
12.	Enter: **<return>**	Returns to 'rgy_edit=> prompt.	

Step	Action	Expected Results	Comments
13.	Enter: **do a** to create the account.	Changes to account domain.	
14.	Enter: **a**	Add new account.	Account A.
15.	Enter: <**useridA>**	Add account id.	
16.	Enter: <**group_nameA**>	Add account group name.	Use group name A.
17.	Enter: <**organization_name**>	Account organization.	
18.	Enter: <**new_password**>	Enter password for account.	
19.	Enter: <**new_password**>	Re-enter user password.	
20.	Enter: <**admin_password**>	Enter administration password.	
21.	Enter: <**return>**	Misc. information.	
22.	Enter: <**/home/userid**>	Enter home directory.	
23.	Enter: <**/bin/csh**>	Enter default shell path.	
24.	Enter: **<return>**	Password valid.	Default (yes)
25.	Enter: **<return>**	Expiration date.	Default (none)
26.	Enter: **<return>**	Allow account to be server principal.	Default (yes)
27.	Enter: **<return>**	Allow account to be client principal.	Default (yes)
28.	Enter: **<return>**	Account valid for login.	Default (yes)
29.	Enter: **<return>**	Allow post-dated certificates.	Default (no)
30.	Enter: **<return>**	Allow forwardable certificates.	Default (yes)
31.	Enter: <**return>**	Permit TGT authentication.	Default (yes)
32.	Enter: **<return>**	Allow renewable certificates.	Default (yes)
33.	Enter: **<return>**	Allow proxiable certificates.	Default (no)
34.	Enter: **<return>**	Allow duplicate session keys.	Default (no)
35.	Enter: **<return>**	Good since date.	Default (current date & time)
36.	Enter: **<return>**	Create/change auto policy for this account.	Default (no)
37.	Enter: **<return>**	Exit from ‘Add Account=>Enter account id (pname):’ prompt	Returns to ‘rgy-edit=>‘ prompt

Step	Action	Expected Results	Comments
38.	Enter: **do p**	Changes to principal domain to enter a new user.	
39.	Enter: **add**	Adds a new principle name.	
40.	Enter: <**user_idB>**	Enter user id of new user.	
41.	Enter: <**unix_ID_number>**	This is the number retrieved from the passwd file in step 2.	
42.	Enter full name of user.	Associates the user's full name to the user id.	
43.	Enter: **<return>**	Use default value for object creation quota.	
44.	Enter: **<return>**	Returns to 'rgy_edit=> prompt.	
45.	Enter: **do a** to create the account.	Changes to account domain.	
46.	Enter: **a**	Add new account.	Account B.
47.	Enter: <**useridB>**	Add account id.	
48.	Enter: <**group_nameA**>	Add account group name.	Use group name A.
49.	Enter: <**organization_name**>	Account organization.	
50.	Enter: <**new_password**>	Enter password for account.	
51.	Enter: <**new_password**>	Re-enter user password.	
52.	Enter: <**admin_password**>	Enter administration password.	
53.	Enter: <**return>**	Misc. information.	
54.	Enter: </**home/userid**>	Enter home directory.	
55.	Enter: </**bin/csh**>	Enter default shell path.	
56.	Enter: **<return>**	Password valid.	Default (yes)
57.	Enter: **<return>**	Expiration date.	Default (none)
58.	Enter: **<return>**	Allow account to be server principal.	Default (yes)
59.	Enter: **<return>**	Allow account to be client principal.	Default (yes)
60.	Enter: **<return>**	Account valid for login.	Default (yes)
61.	Enter: **<return>**	Allow post-dated certificates.	Default (no)

Step	Action	Expected Results	Comments
62.	Enter: **<return>**	Allow forwardable certificates.	Default (yes)
63.	Enter: <**return**>	Permit TGT authentication.	Default (yes)
64.	Enter: **<return>**	Allow renewable certificates.	Default (yes)
65.	Enter: **<return>**	Allow proxiable certificates.	Default (no)
66.	Enter: **<return>**	Allow duplicate session keys.	Default (no)
67.	Enter: **<return>**	Good since date.	Default (current date & time)
68.	Enter: **<return>**	Create/change auto policy for this account.	Default (no)
69.	Enter: **<return>**	Exit from 'Add Account=>Enter account id (pname):' prompt	Returns to 'rgy-edit=>' prompt
70.	Enter: **do p**	Changes to principal domain to enter a new user.	
71.	Enter: **add**	Adds a new principle name.	
72.	Enter: <**user_idC**>	Enter user id of new user.	
73.	Enter: <**unix_ID_number>**	This is the number retrieved from the passwd file in step 2.	
74.	Enter full name of user.	Associates the user's full name to the user id.	
75.	Enter: **<return>**	Use default value for object creation quota.	
76.	Enter: **<return>**	Returns to 'rgy_edit=> prompt.	
77.	Enter: **do a** to create the account.	Changes to account domain.	
78.	Enter: **a**	Add new account.	Account C.
79.	Enter: <**useridC**>	Add account id.	
80.	Enter: <**group_nameA**>	Add account group name.	Use group name A.
81.	Enter: <**organization_name**>	Account organization.	

Step	Action	Expected Results	Comments
82.	Enter: <**new_password**>	Enter password for account.	
83.	Enter: <**new_password**>	Re-enter user password.	
84.	Enter: <**admin_password**>	Enter administration password.	
85.	Enter: <**return**>	Misc. information.	
86.	Enter: </**home/userid**>	Enter home directory.	
87.	Enter: </**bin/csh**>	Enter default shell path.	
88.	Enter: **<return>**	Password valid.	Default (yes)
89.	Enter: **<return>**	Expiration date.	Default (none)
90.	Enter: **<return>**	Allow account to be server principal.	Default (yes)
91.	Enter: **<return>**	Allow account to be client principal.	Default (yes)
92.	Enter: **<return>**	Account valid for login.	Default (yes)
93.	Enter: **<return>**	Allow post-dated certificates.	Default (no)
94.	Enter: **<return>**	Allow forwardable certificates.	Default (yes)
95.	Enter: <**return**>	Permit TGT authentication.	Default (yes)
96.	Enter: **<return>**	Allow renewable certificates.	Default (yes)
97.	Enter: **<return>**	Allow proxiable certificates.	Default (no)
98.	Enter: **<return>**	Allow duplicate session keys.	Default (no)
99.	Enter: **<return>**	Good since date.	Default (current date & time)
100.	Enter: **<return>**	Create/change auto policy for this account.	Default (no)
101.	Enter: **<return>**	Exit from 'Add Account=>Enter account id (pname):' prompt	Returns to 'rgy-edit=>' prompt
102.	Enter: **do p**	Changes to principal domain to enter a new user.	
103.	Enter: **add**	Adds a new principle name.	

Step	Action	Expected Results	Comments
104.	Enter: <**user_idD>**	Enter user id of new user.	
105.	Enter: <**unix_ID_number>**	This is the number retrieved from the passwd file in step 2.	
106.	Enter full name of user.	Associates the user's full name to the user id.	
107.	Enter: **<return>**	Use default value for object creation quota.	
108.	Enter: **<return>**	Returns to 'rgy_edit=> prompt.	
109.	Enter: **do a** to create the account.	Changes to account domain.	
110.	Enter: **a**	Add new account.	Account D.
111.	Enter: <**useridD>**	Add account id.	
112.	Enter: <**group_nameA**>	Add account group name.	Use group name A.
113.	Enter: <**organization_name**>	Account organization.	
114.	Enter: <**new_password**>	Enter password for account.	
115.	Enter: <**new_password**>	Re-enter user password.	
116.	Enter: <**admin_password**>	Enter administration password.	
117.	Enter: <**return>**	Misc. information.	
118.	Enter: </**home/userid**>	Enter home directory.	
119.	Enter: </**bin/csh**>	Enter default shell path.	
120.	Enter: **<return>**	Password valid.	Default (yes)
121.	Enter: **<return>**	Expiration date.	Default (none)
122.	Enter: **<return>**	Allow account to be server principal.	Default (yes)
123.	Enter: **<return>**	Allow account to be client principal.	Default (yes)
124.	Enter: **<return>**	Account valid for login.	Default (yes)
125.	Enter: **<return>**	Allow post-dated certificates.	Default (no)
126.	Enter: **<return>**	Allow forwardable certificates.	Default (yes)
127.	Enter: <**return>**	Permit TGT authentication.	Default (yes)
128.	Enter: **<return>**	Allow renewable certificates.	Default (yes)
129.	Enter: **<return>**	Allow proxiable	Default (no)

Step	Action	Expected Results	Comments
		certificates.	
130.	Enter: <**return**>	Allow duplicate session keys.	Default (no)
131.	Enter: <**return**>	Good since date.	Default (current date & time)
132.	Enter: <**return**>	Create/change auto policy for this account.	Default (no)
133.	Enter: <**return**>	Exit from 'Add Account=>Enter account id (pname):' prompt	Returns to 'rgy-edit=>' prompt
134.	Enter: **v <useridA>**	Displays Account A information.	Verify all information is as entered.
135.	Enter: **v <useridB>**	Displays Account B information.	Verify all information is as entered.
136.	Enter: **v <useridC>**	Displays Account C information.	Verify all information is as entered.
137.	Enter: **v <useridD>**	Displays Account D information.	Verify all information is as entered.
138.	Using a different workstation verify that each of the accounts is operable by logging onto the system and then logging off.	Access granted. Account A _____ Account B _____ Account C _____ Account D _____	
139.	Back at the work station with the rgy_edit prompt enter: <**do p**>	Changes prompt to principal domain.	
140.	Enter <**delete userid**> where userid is the user id for Account D.	The user is deleted.	
141.	Enter: <**return**>	Return to rgy_edit prompt.	
142.	At another workstation, try to log onto the system using the account just deleted.	Access denied.	
143.	Back at the workstation with the rgy_edit prompt enter: <**do a**>	Changes prompt to account domain.	

Step	Action	Expected Results	Comments
144.	Enter: **c -p <principlename> -g <groupname> -o <orgname> -pw <newpasswd> -mp <adminpasswd>**	Change Account A password.	Principle name is the same as the user name.
145.	Enter: **v <username_Account A>**	Displays information about user A.	Verify that the password has been changed.
146.	Enter: <**return**>	Exits the rgy_edit prompt.	
147.	Logon to the system using Account A with new password.	Access granted.	

Post Test Analysis:

Step	Analysis Required	Expected Results	Comments
1.	Examine history log and ensure all steps from the test case were recorded.	All functions performed should be recorded.	

SFT04.2 User Group Specification

This test case addresses the management of user groups within the system.

Step	Action	Expected Results	Comments
1.	Log on to the Ir1 DCE Host in the EDF as a DCE cell administrator. Enter: **telnet dceserver** - or - **rsh dceserver**	Access to system granted.	
2.	Enter: **dce_login_cell_admin**	Logs in to DCE as cell administrator.	
3.	Enter: **<admin_password>**	Password accepted.	
4.	Enter: **rgy_edit**	Brings up the DCE registry edit tool.	
5.	Enter: <**do a**>	Changes prompt to account domain.	

Step	Action	Expected Results	Comments
6.	Enter: **c -p <UsernameB> -g <newgroupname>**	Change Account B group.	
7.	Enter: **c -p <UsernameC> -g <newgroupname>**	Change Account C group.	
8.	Enter: **v <useridA>**	Displays Account A information.	
9.	Enter: **v <useridB>**	Displays Account B information - verify that the group name is different between A and B.	
10.	Enter: **v <useridC>**	Displays Account C information - verify that the group name is different from A and B.	
11.	Enter: **exit**	Exits the rgy_edit prompt.	

Post Test Analysis:

Step	Analysis Required	Expected Results	Comments
1.	Examine history log and ensure all steps from the test case were recorded.	All functions performed should be recorded.	

SFT04.3 User Privilege Authentication

This test case ensures that the specified user privileges are implemented by the system.

Step	Action	Expected Results	Comments
1.	Log on to the system using one of the three accounts created in this thread.	Access to system.	
2.	Perform functions within the scope of the privileges assigned to the user account.	All functions are performed.	
3.	Attempt to perform functions outside of the privileges assigned to the user account.	Warning messages displayed. Updates made to the history log showing attempted operations. Operations are not performed.	

Step	Action	Expected Results	Comments
4.	Repeat test case with other two accounts generated in SFT04.1.	Operations performed with proper privileges. Other operations are not performed.	

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Compare history log against operations performed in steps 2 and 3 for each account.	The history log should contain entries for each function performed or attempted.	

SFT04.4 Security Fault Detection and Response

This test case addresses the detection and response to unauthorized access to the system.

Step	Action	Expected Results	Comments
1.	Attempt to log into the local system using invalid account names.	Access denied, invalid attempts logged.	
2.	Attempt to log into a remote system using invalid account names.	Access denied, invalid attempts logged.	
3.	Repeat the attempted login process until the system is compromised and the system shuts out the user's attempt to log in.	Alarm generated at the SMC station to alert that the system security is being compromised. The alert should include the location of the attempt.	
4.	Print the security logs and associated reports.	Each invalid attempt is printed to the security logs and included in the security reports.	

Post Test Analysis:

Step	Action	Expected Results	Comments
1.	Examine the security logs and the security reports.	All login attempts from steps 1 and 2 should be contained in both the security logs and the security reports.	

Test Termination:

Step	Action	Expected Results	Comments
1.	Delete all accounts created for this test.	Accounts deleted.	
2.	Log off the ECS.	Return to UNIX prompt.	
3.	Enter: **ctrl-D** to halt the script command.	Operator commands no longer logged.	
4.	Enter: **lpr -P** <printer name> <filename>	The history log is printed.	

4.10 SFT05 - ECS Standard Services

Test Objectives:

This test verifies the availability of system standard services on the various system workstations. Specific objectives to be tested are:

- Availability of SDP Toolkit at AI&T workstation.
- Availability of Standard Services at the user workstation.

Test Configuration:

- Hardware: AI&T Workstation, Ingest Workstation
- Software: SDPTK, DCCI CSCIs.
- Test Tools: None.

Test Data:

None.

Requirements Verified:

Mission Essential:
EOSD0502 ESN-0003 ESN-0010 ESN-1170 PGS-0602

Mission Fulfillment:
None.
Procedures:

Test Set-up:

Step	**Action**	**Expected Results**	**Comments**
1.	Acquire files to compile with and without errors (C++, FORTRAN, and Ada).	Record file names/path: FORTRAN No error: _____ Errors: _____ C++ No error: _____ Errors: _____ Ada No error: _____ Errors: _____	All files for this test thread will be either supplied by HAIS, generated by the test team, or obtained from other sources.
2.	Acquire two sets of files to compare: one set identical, one set with differences.	Record file names/path: Identical: _____ _____ Differences: _____ _____	
3.	Acquire a files to use the code checker on.	File name/path compliant with code checker: _____ File not compliant: _____	
4.	Acquire a document to utilize the viewing tool.	File name/path: _____	

Step	Action	Expected Results	Comments
5.	Acquire a product to utilize the visualization / graphic tool.	File name/path: _____	
6.	Start a UNIX script file to record test activities. Enter: **script** <filename>	Script file is started, record filename here: _____	

Test Execution:

SFT05.1 SDP Toolkit Availability

This test case verifies the availability of standard toolkit services at the user workstations. The test is repeated on both hardware platforms at each DAAC. The following compilers are being delivered at the indicated DAAC:

DAAC	C++	FORTRAN 77	Ada
EDC		X	
GSFC	X	X	
LaRC	X	X	X
MSFC	X	X	

Therefore, only the test associated with the compilers at the DAAC being tested need to be executed. Utilizing the Ada compiler at EDC will not work so that test step can be omitted when testing the EDC DAAC.

Step	Action	Expected Results	Comments
1.	Logon to an AI&T workstation.	Access granted.	
2.	Enter: **cd <test_data directory>**	Set working directory to location of data to execute this test.	
3.	Enter: **setenv FC f77**	Sets environment to compile FORTRAN 77 files.	
4.	Enter: **f77 <filename77.f>**	Compiles FORTRAN file successfully.	File information is in test set up step 1.
5.	Enter: **f77 <error_filename77.f>**	Compile errors detected.	File information is in test set up step 1.
6.	Enter: **cc -Xc**	Compile C file	File information is in

Step	Action	Expected Results	Comments
	<filename.c> -o no_error.out	successfully.	test set up step 1.
7.	Enter: **cc -Xc <error_filename.c> -o error.out**	Compiles errors detected.	File information is in test set up step 1.
8.	Enter: **ada -M <filename.a>**	Compiles Ada file successfully.	File information is in test set up step 1.
9.	Enter: **ada -M <error_filename.a>**	Compile errors detected.	File information is in test set up step 1.
10.	Enter: **SSIT Manager <DpAtMgr>**	Invokes GUI.	
11.	Click the 'Tools' option from the pull down menu.	Tools menu is displayed.	
12.	Click option for 'Product Examination'	Contents of Production Examination Menu is displayed.	
13.	Click option for 'File Comparison'	The menu of File Comparison is displayed.	
14.	Click button 'File #1' and enter the file name of the first identical file.	Information entered for file 1.	File information listed in test set-up step 2.
15.	Click button 'File #2' and enter the file name of the second identical file.	Information entered for file 2.	File information listed in test set-up step 2.
16.	Click on report to save the results to a file.		
17.	Click on 'Compare' to compare the two files.	No differences found.	
18.	Click option for 'File Comparison'	The menu of File Comparison is displayed.	
19.	Click button 'File #1' and enter the file name of the first file.	Information entered for file 1.	File information listed in test set-up step 2.
20.	Click button 'File #2' and enter the file name of the second file which contains differences.	Information entered for file 2.	File information listed in test set-up step 2.
21.	Click on report to save the results to a file.		
22.	Click on 'Compare' to compare the two files.	Differences found and reported.	
23.	Click on the 'Tools' button from the menu.	Tools menu is displayed.	

Step	Action	Expected Results	Comments
24.	Click the Standards Checkers button.	Standards Checkers Menu is displayed.	
25.	Click the Prohibited Function Checker button.	Prohibited Function Checker menu is displayed.	
26.	Click the Analyze button.	The file selector menu is displayed.	
27.	Select the file listed in test set-up step 3 with no errors.	The file is analyzed and found compliant.	
28.	Click the Analyze button.	The file selector menu is displayed.	
29.	Select the file listed in test set-up step 3 with known compliance errors.	The compliant errors are found and reported on.	
30.	Click the print button.	Report of compliance violation printed.	
31.	Click on the 'Tools' option.	Tools menu is displayed.	
32.	Click option for Office Automation.	Office Automation menu is displayed.	
33.	Click on the MSWindows option.	MSWindow's Program Manager is displayed.	
34.	Click on Microsoft Word.	Microsoft Word program is displayed.	
35.	Click on the file button.	File menu is displayed.	
36.	Select the file to be viewed.	File contents is displayed.	File path/name is listed in test set-up step 4.
37.	Select the print option.	File is printed.	
38.	Click on the Product Examination button.	Product examination menu is displayed.	
39.	Click on the EOSView button.	EOSView program is displayed.	
40.	Using the file pull down menu, select the file to display.	File is opened and displayed.	File path/name is listed in test set-up step 5.
41.	Using the files pull down menu, quit the SSI&T manager.	Returns user to UNIX prompt.	

Post Test Analysis

Step	Action	Expected Results	Comments

1.	Examine history log.	All functions utilized during the test appear in the history log in sequence.	

SFT05.2 ECS Standard Services Availability

This test case verifies the availability of ECS standard services at the user workstations.

Step	Action	Expected Results	Comments
1.	Log on to the workstation under test.	Access granted.	
2.	Enter: **mail <**userid at EDF@mail address><userid at GSFC@mail address><userid at LaRC@mail address><userid at EDC@mail address><userid at MSFC@mail address> and hit enter key.	Enter the mail system and wait for the message text to be entered.	
3.	Type the message text to send to all DAAC sites and the EDF.	The message is displayed on the screen as it is entered.	
4.	Enter: **'.'** to send the message.	Message sent to all DAAC sites.	
5.	Log onto the bulletin board server workstation at the DAAC and enter: **xvnews &**	Bulletin board service is initialized.	
6.	Click on the 'view groups' button.	Various bulletin boards are displayed.	
7.	Click on one of the bulletin boards.	the name of the bulletin board is added to a list in the bottom window.	
8.	Click on the 'subscribe' button.	The status is updated from 'unsubscribed' to 'subscribe'.	
9.	Click on 'done' button.	A list of bulletin boards currently subscribed to are displayed.	

Step	Action	Expected Results	Comments
10.	Click on one of the subscribed bulletin boards.	The bulletin board name is highlighted.	
11.	Click on 'read group' button.	A list of postings are displayed at the top of the window.	
12.	Click on any of the postings to open them for reading.	The selected posting is displayed.	
13.	With the right mouse button, click on the 'Post/E-mail; button, followed by 'Post follow up'.	A post follow-up window appears with a mail message to be posted back to the bulletin board.	
14.	Enter a reply to the message.	Message is entered.	
15.	Click on the 'post reply' button to send the reply to the bulletin board.	The message is added to the bulletin board.	
16.	Click on the 'quit' button to close.	Exits the bulletin board service.	
17.	Enter: **Mosaic &**	The NCSA Mosaic: Open Document is displayed.	
18.	Enter the URL address: **http://fairmont.ivv.nasa.gov/**	The NASA IV&V home page is displayed.	
19.	Use the mouse to view different items on the IV&V homepage.	Selected items are displayed.	
20.	Use the file pull down menu to quit Mosaic.	The Mosaic program terminates.	

Post Test Analysis

No post test analysis is necessary for this test.

Test Termination:

Step	Action	Expected Results	Comments
1.	Log off the ECS.	Return to UNIX prompt.	
2.	Enter: **ctrl-D** to halt the script command.	Operator commands no longer logged.	
3.	Enter: **lpr -P** <printer name> <filename>	The history log is printed.	